

FIG. 1

09/830392

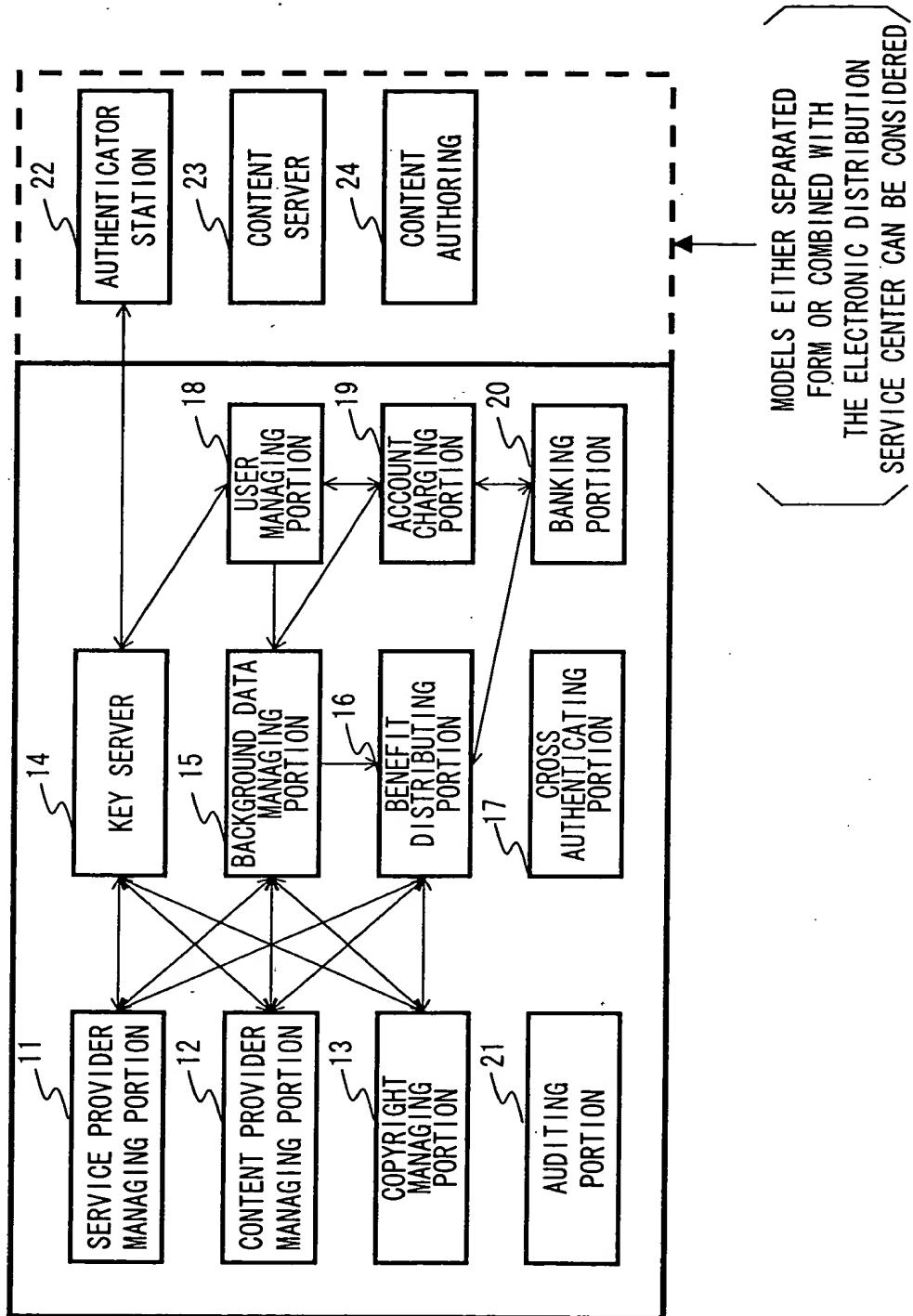
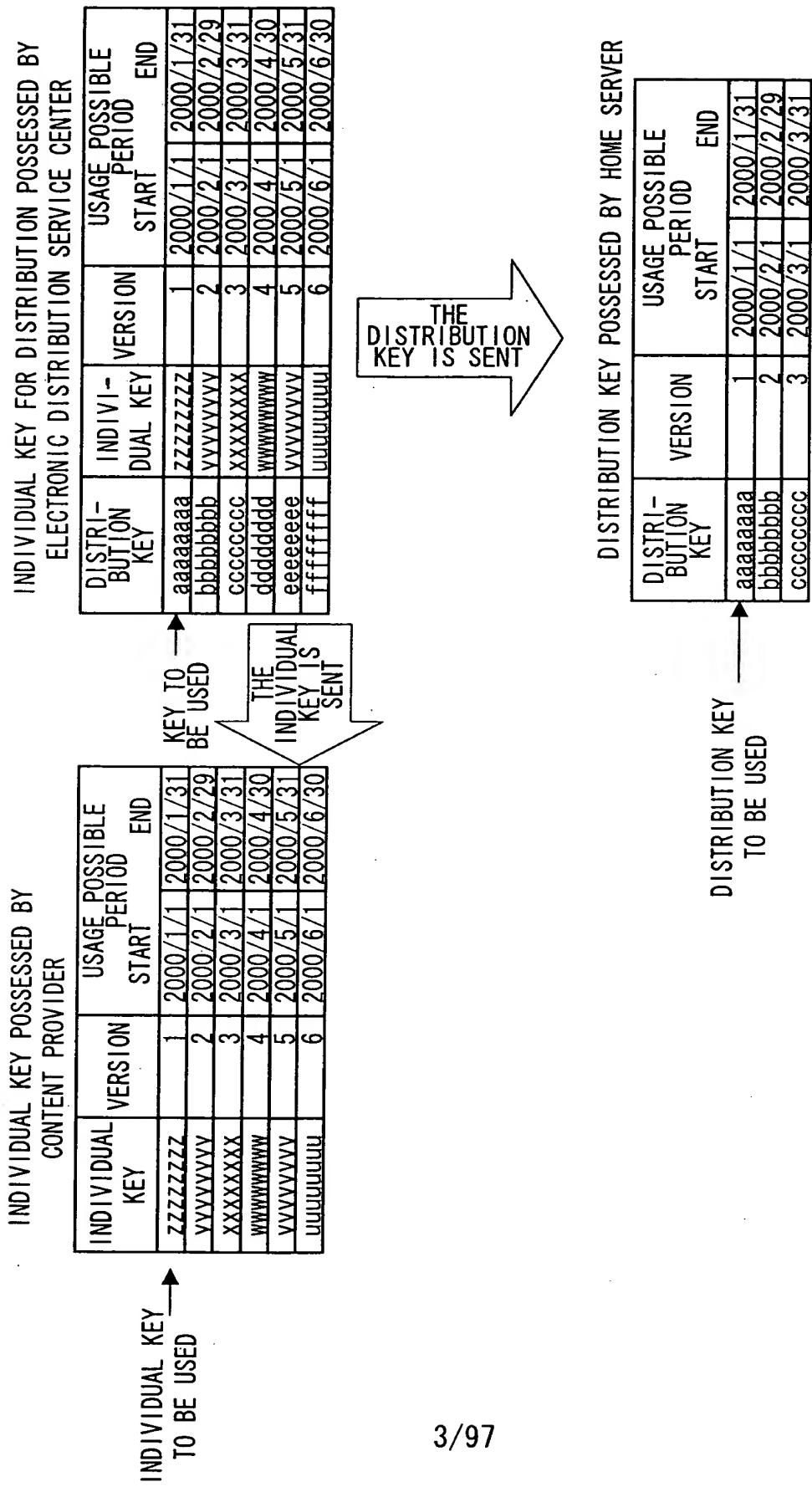


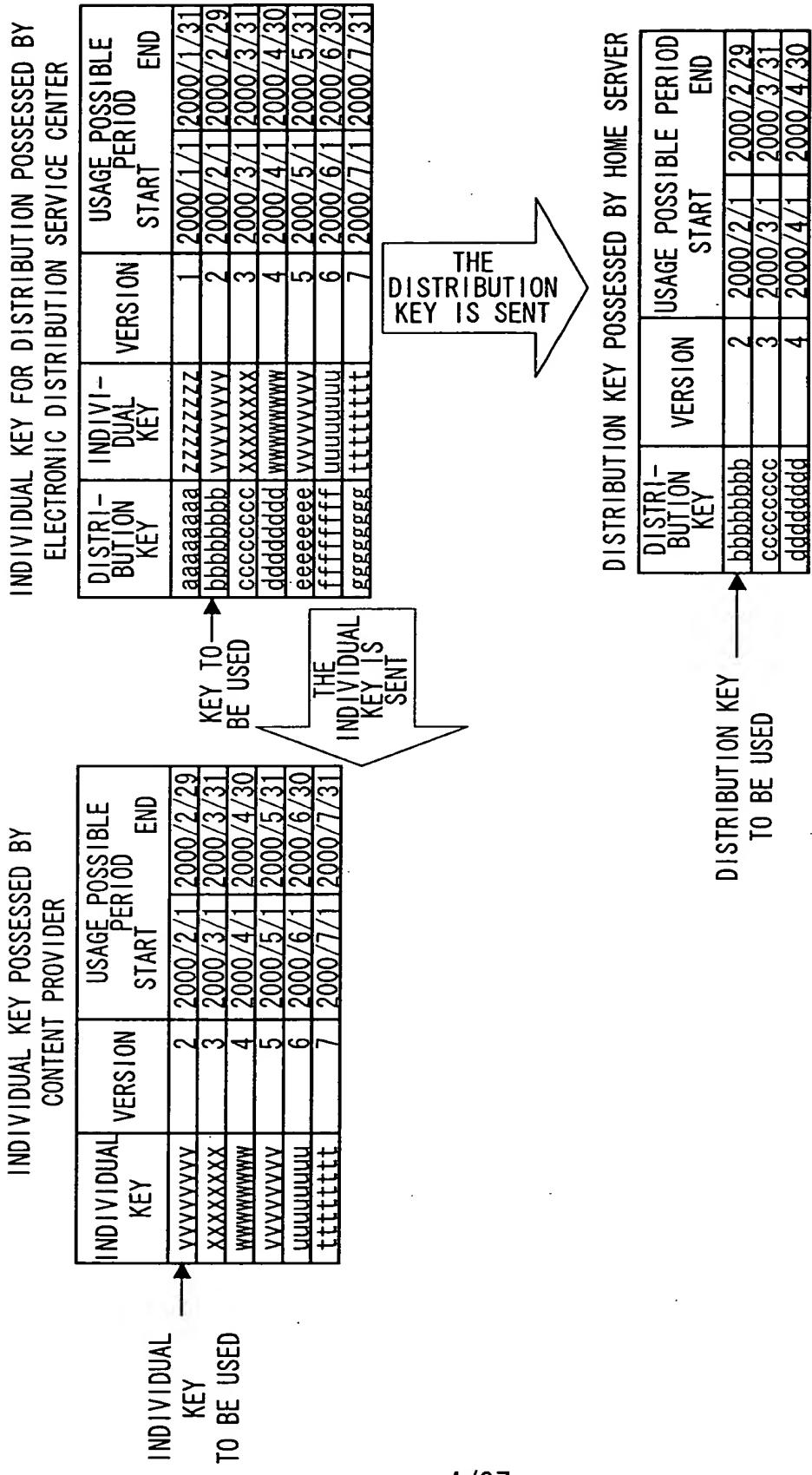
FIG. 2

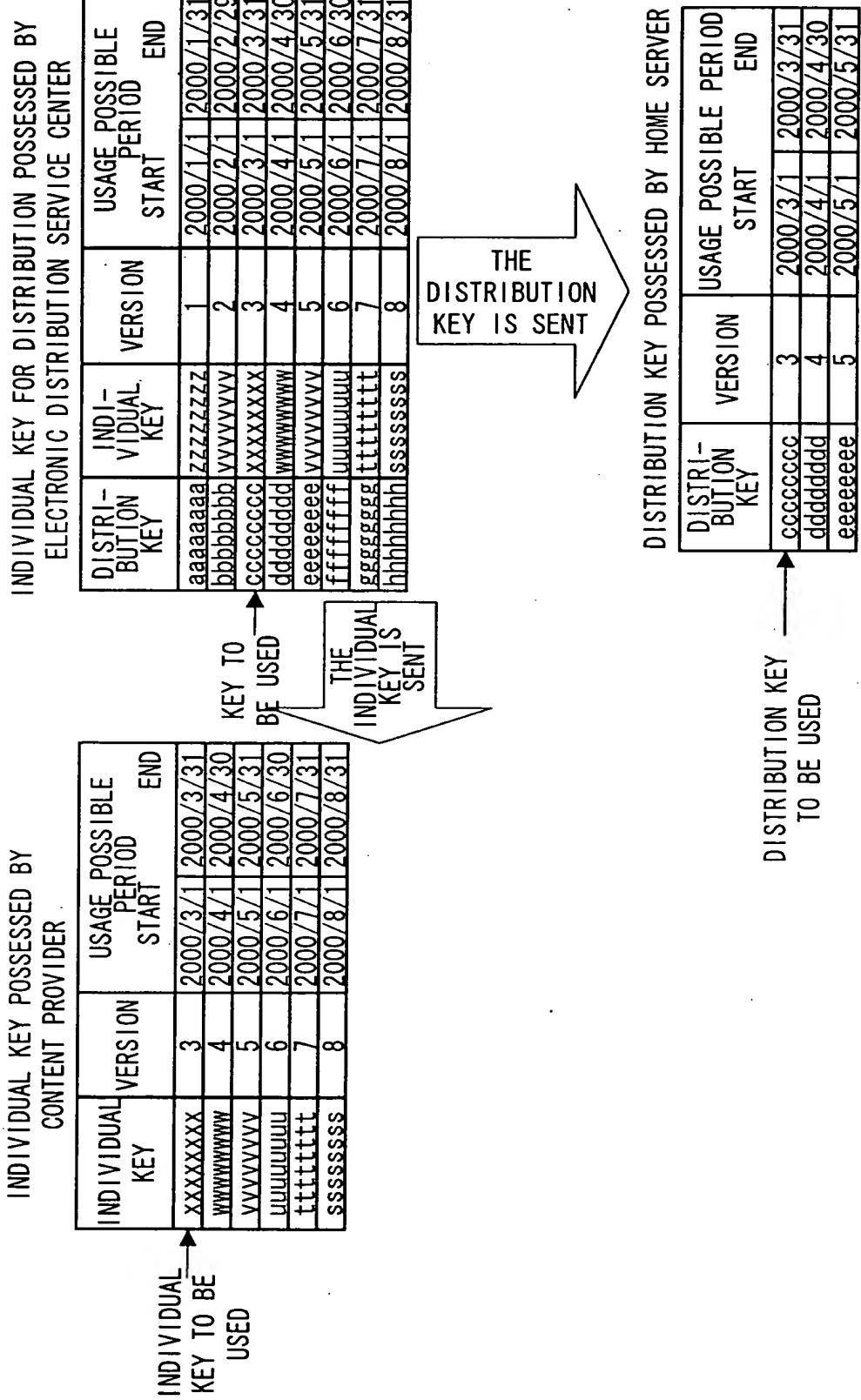
09/830392



TO GET GO "26 E 0 E 0 6 0

09/830392





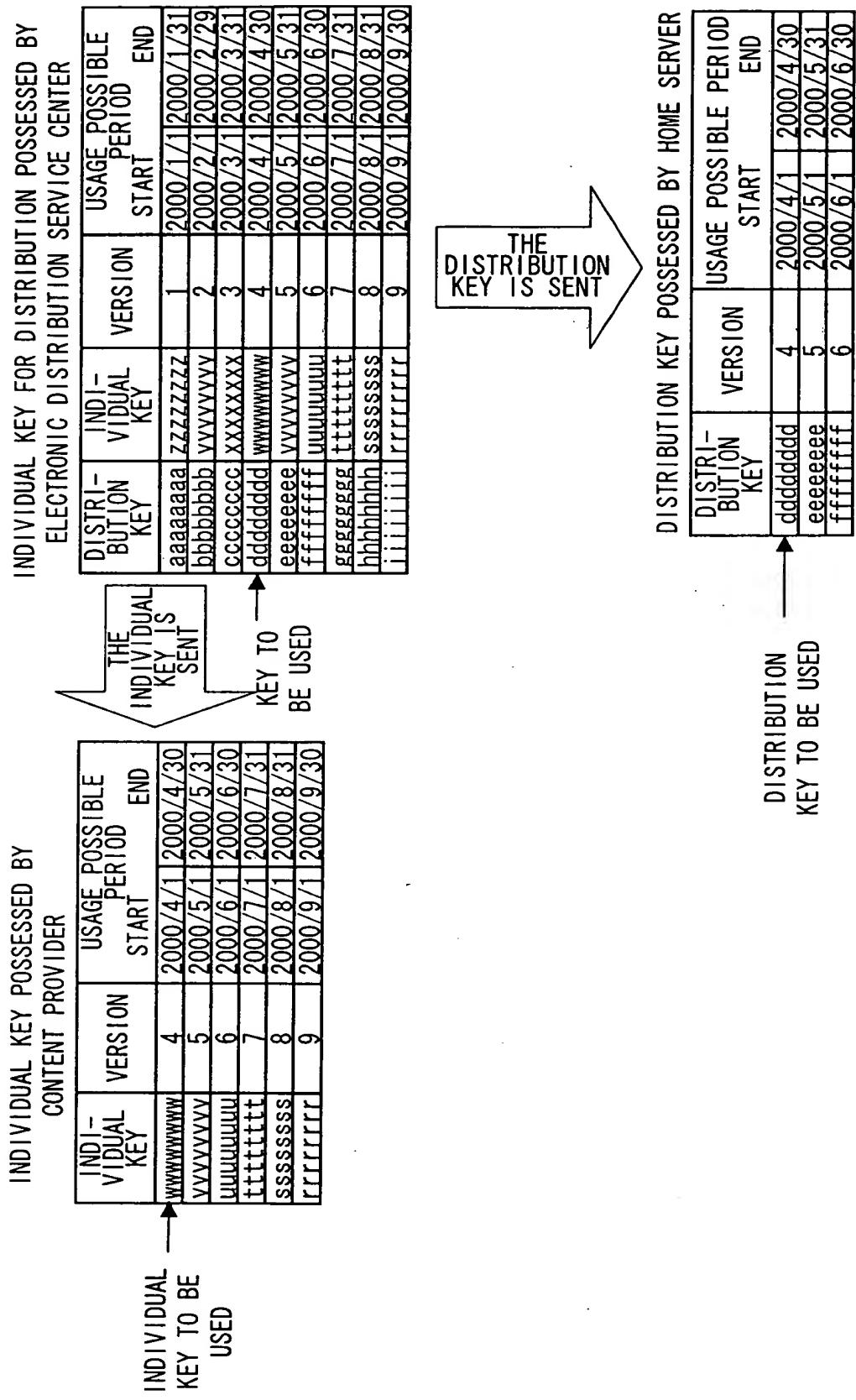


FIG. 6

09/830392

GROUP ID	ID	CONNECTION TO SERVICE CENTER	SETTLEMENT PROCESSING	PURCHASE PROCESSING	PROXY PAYER	PROXY PURCHASER	REGISTRATION
Gp ID1	ID1	POSSIBLE	POSSIBLE	POSSIBLE	—	—	POSSIBLE
	ID2	POSSIBLE	NOT POSSIBLE	POSSIBLE	ID1	—	POSSIBLE
	ID3	POSSIBLE	NOT POSSIBLE	POSSIBLE	ID1	—	NOT POSSIBLE
	ID4	NOT POSSIBLE	NOT POSSIBLE	NOT POSSIBLE	—	ID1	POSSIBLE
	ID5	NOT POSSIBLE	NOT POSSIBLE	NOT POSSIBLE	—	ID2	NOT POSSIBLE
Gp ID2	ID6	POSSIBLE	POSSIBLE	POSSIBLE	—	—	NOT POSSIBLE
	ID7	POSSIBLE	NOT POSSIBLE	POSSIBLE	—	—	NOT POSSIBLE
	ID8	POSSIBLE	NOT POSSIBLE	POSSIBLE	ID6	—	NOT POSSIBLE
	ID9	NOT POSSIBLE	NOT POSSIBLE	NOT POSSIBLE	—	ID6, 7, 8	NOT POSSIBLE
	ID10	NOT POSSIBLE	NOT POSSIBLE	NOT POSSIBLE	—	ID6, 7, 8	NOT POSSIBLE
Gp ID3	ID11	POSSIBLE	POSSIBLE	POSSIBLE	—	—	NOT POSSIBLE
	ID12	POSSIBLE	NOT POSSIBLE	POSSIBLE	ID11	—	NOT POSSIBLE
	ID13	POSSIBLE	NOT POSSIBLE	POSSIBLE	ID11	—	POSSIBLE
	ID14	NOT POSSIBLE	NOT POSSIBLE	NOT POSSIBLE	—	ID11, 12, 13	NOT POSSIBLE
	ID15	NOT POSSIBLE	NOT POSSIBLE	NOT POSSIBLE	—	ID11	POSSIBLE

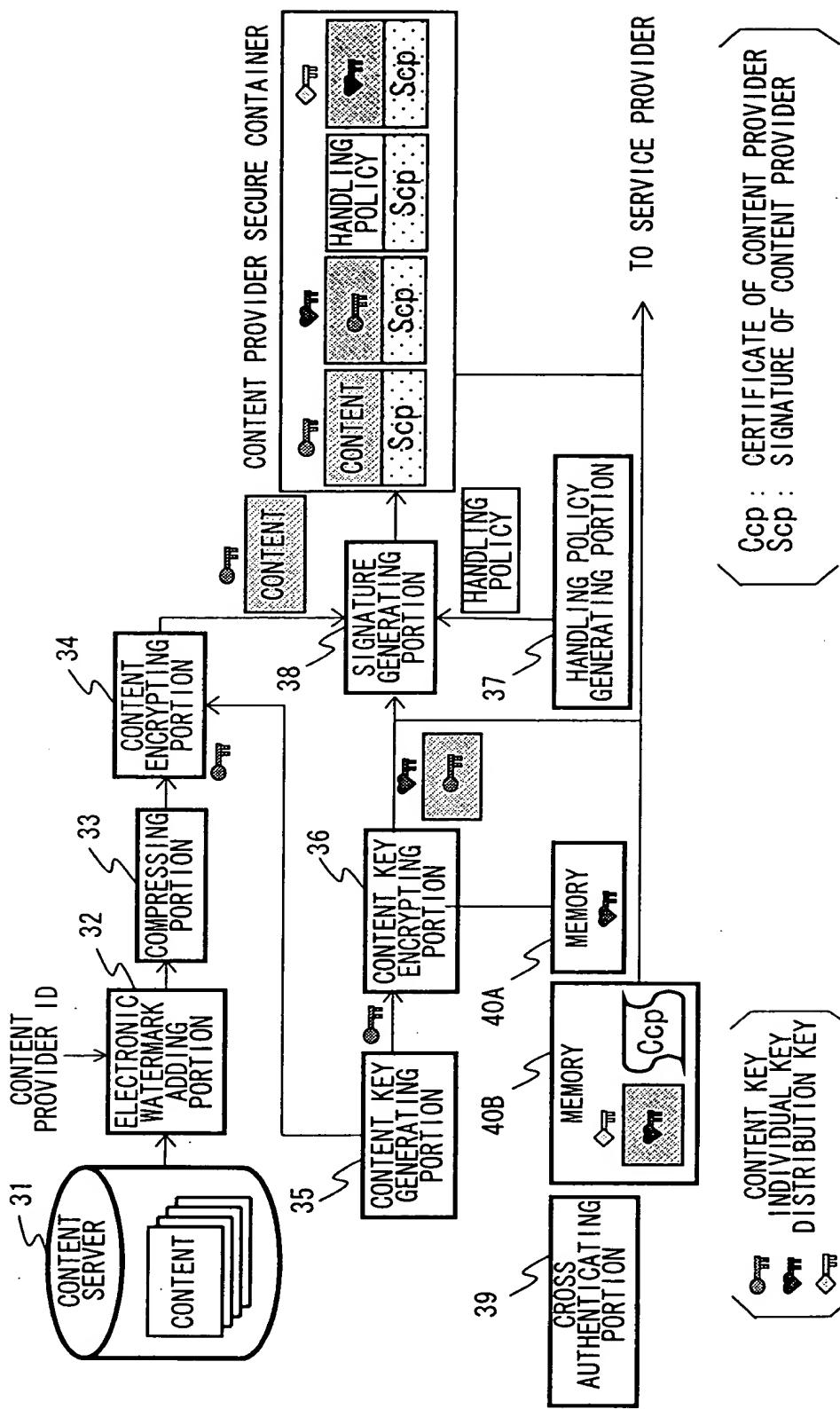
09/830392

GROUP ID	1 D CONNECTION TO SERVICE CENTER	SETTLEMENT PROCESSING	SETTLEMENT ID	PURCHASE PROCESSING	PROXY PAYER	PROXY PURCHASER	REGISTRATION	SIG-NATURE
(A) Gp1	D1 POSSIBLE	POSSIBLE	SETTLEMENT ID 1	POSSIBLE	—	—	POSSIBLE	SIG-NATURE
	D2 POSSIBLE	NOT POSSIBLE	—	POSSIBLE	D1	—	POSSIBLE	SIG-NATURE
	D3 POSSIBLE	NOT POSSIBLE	—	POSSIBLE	D1	—	NOT POSSIBLE	SIG-NATURE
	D4 NOT POSSIBLE	NOT POSSIBLE	—	NOT POSSIBLE	—	D1	POSSIBLE	SIG-NATURE
	D5 NOT POSSIBLE	NOT POSSIBLE	—	NOT POSSIBLE	—	D2	NOT POSSIBLE	SIG-NATURE

(A)

GROUP ID	1 D CONNECTION TO SERVICE CENTER	SETTLEMENT PROCESSING	SETTLEMENT ID	PURCHASE PROCESSING	PROXY PAYER	PROXY PURCHASER	REGISTRATION	SIG-NATURE
(B) Gp2	D6 POSSIBLE	POSSIBLE	SETTLEMENT ID 2	POSSIBLE	—	—	POSSIBLE	SIG-NATURE
	D7 POSSIBLE	NOT POSSIBLE	—	POSSIBLE	D6	—	POSSIBLE	SIG-NATURE
	D8 POSSIBLE	NOT POSSIBLE	—	POSSIBLE	D6	—	NOT POSSIBLE	SIG-NATURE
	D9 NOT POSSIBLE	NOT POSSIBLE	—	NOT POSSIBLE	—	D6	POSSIBLE	SIG-NATURE
	D10 NOT POSSIBLE	NOT POSSIBLE	—	NOT POSSIBLE	—	D6	7 8	NOT POSSIBLE

(B)



## (SIGNATURE GENERATION)

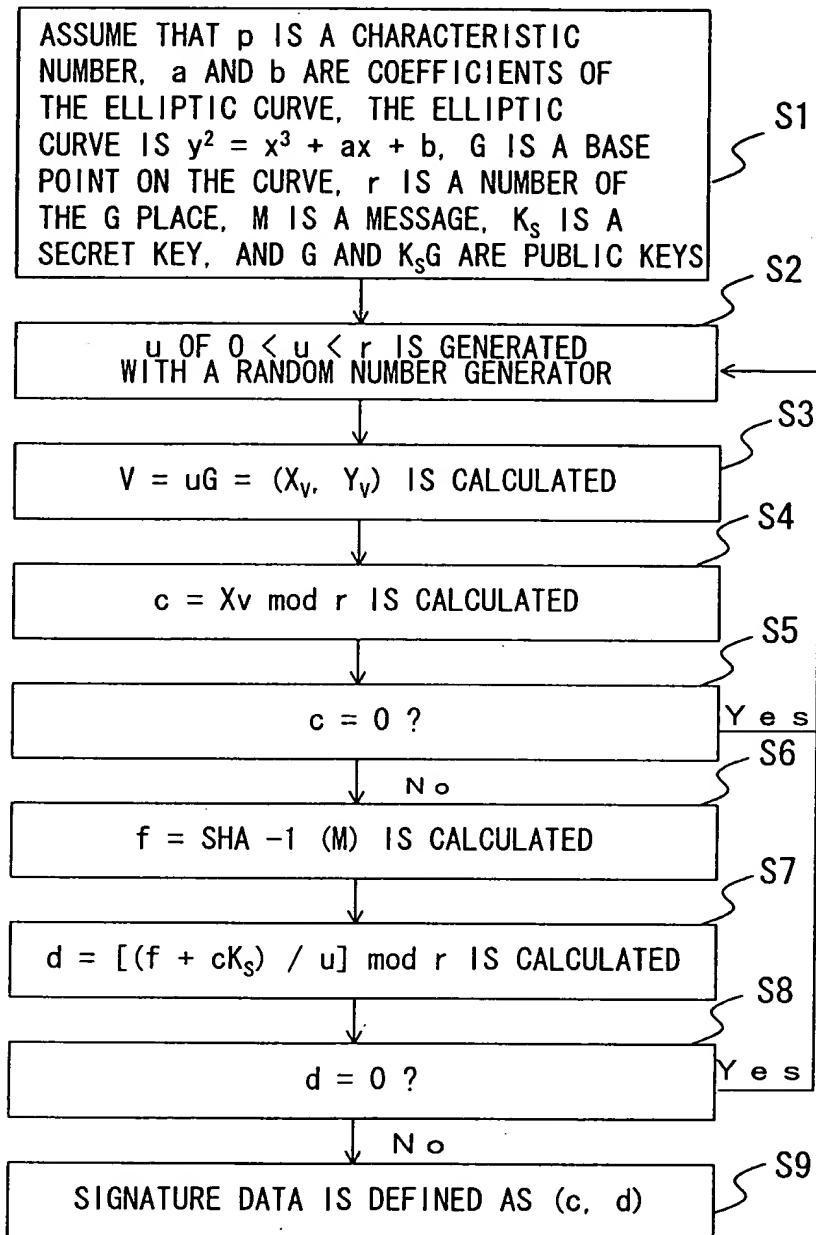


FIG. 10

## (SIGNATURE VERIFICATION)

ASSUME THAT  $p$  IS A CHARACTERISTIC NUMBER,  $a$  AND  $b$  ARE COEFFICIENTS OF THE ELLIPTIC CURVE, THE ELLIPTIC CURVE IS  $y^2 = x^3 + ax + b$ ,  $G$  IS A BASE POINT ON THE CURVE,  $r$  IS A NUMBER OF THE  $G$  PLACE,  $M$  IS A MESSAGE,  $(c, d)$  IS A SIGNATURE AND  $G$  AND  $K_S G$  ARE PUBLIC KEYS

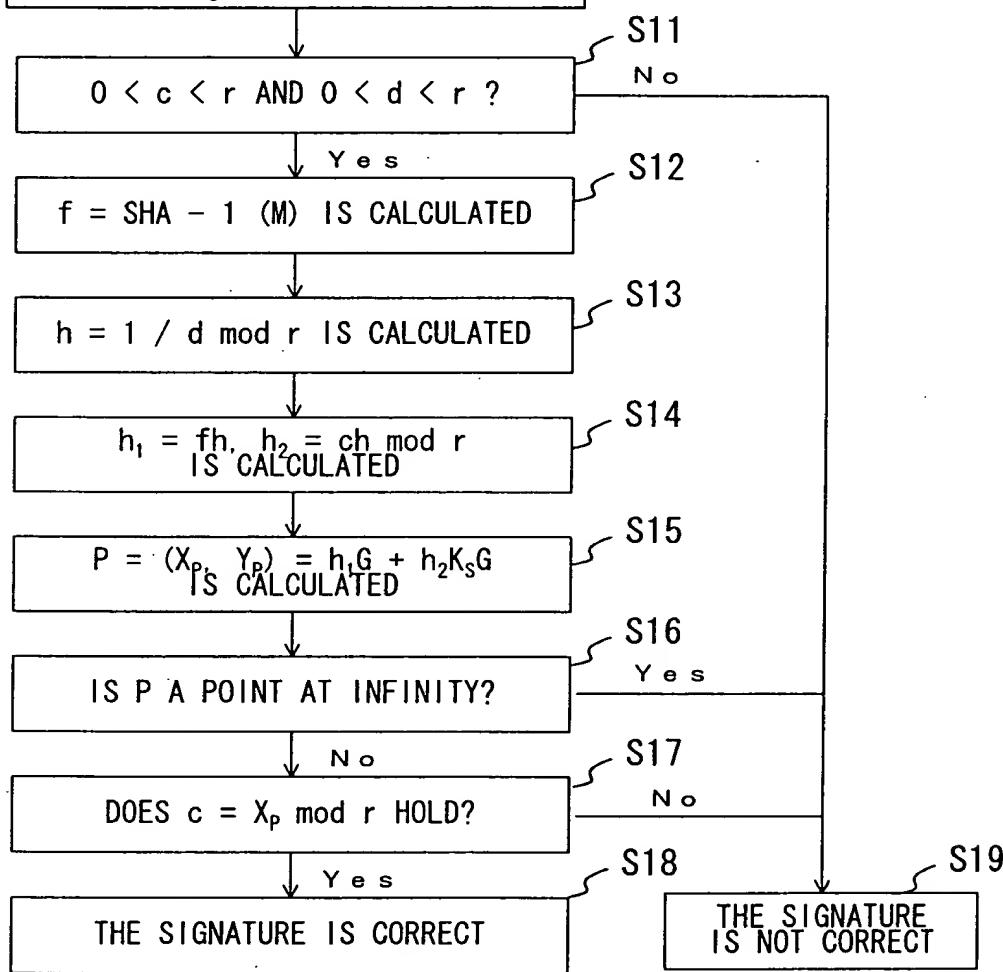


FIG. 11

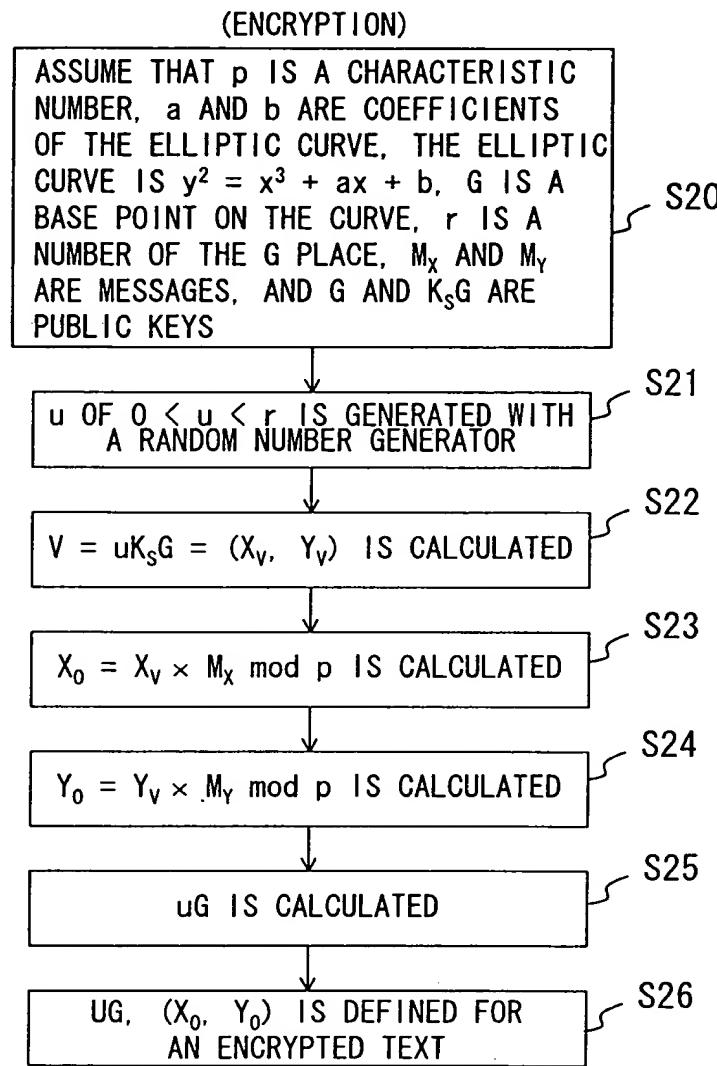


FIG. 12

## (DECRYPTION)

ASSUME THAT  $p$  IS A CHARACTERISTIC NUMBER,  $a$  AND  $b$  ARE COEFFICIENTS OF THE ELLIPTIC CURVE, THE ELLIPTIC CURVE IS  $y^2 = x^3 + ax + b$ ,  $G$  IS A BASE POINT ON THE CURVE,  $r$  IS A NUMBER OF THE  $G$  PLACE,  $uG$  AND  $(X_0, Y_0)$  ARE ENCRYPTED TEXTS, AND  $K_{sG}$  IS A PUBLIC KEY

S30

$K_{sG} = (X_v, Y_v)$  IS CALCULATED

S31

$X_1 = X_0/X_v \bmod p$  IS CALCULATED

S32

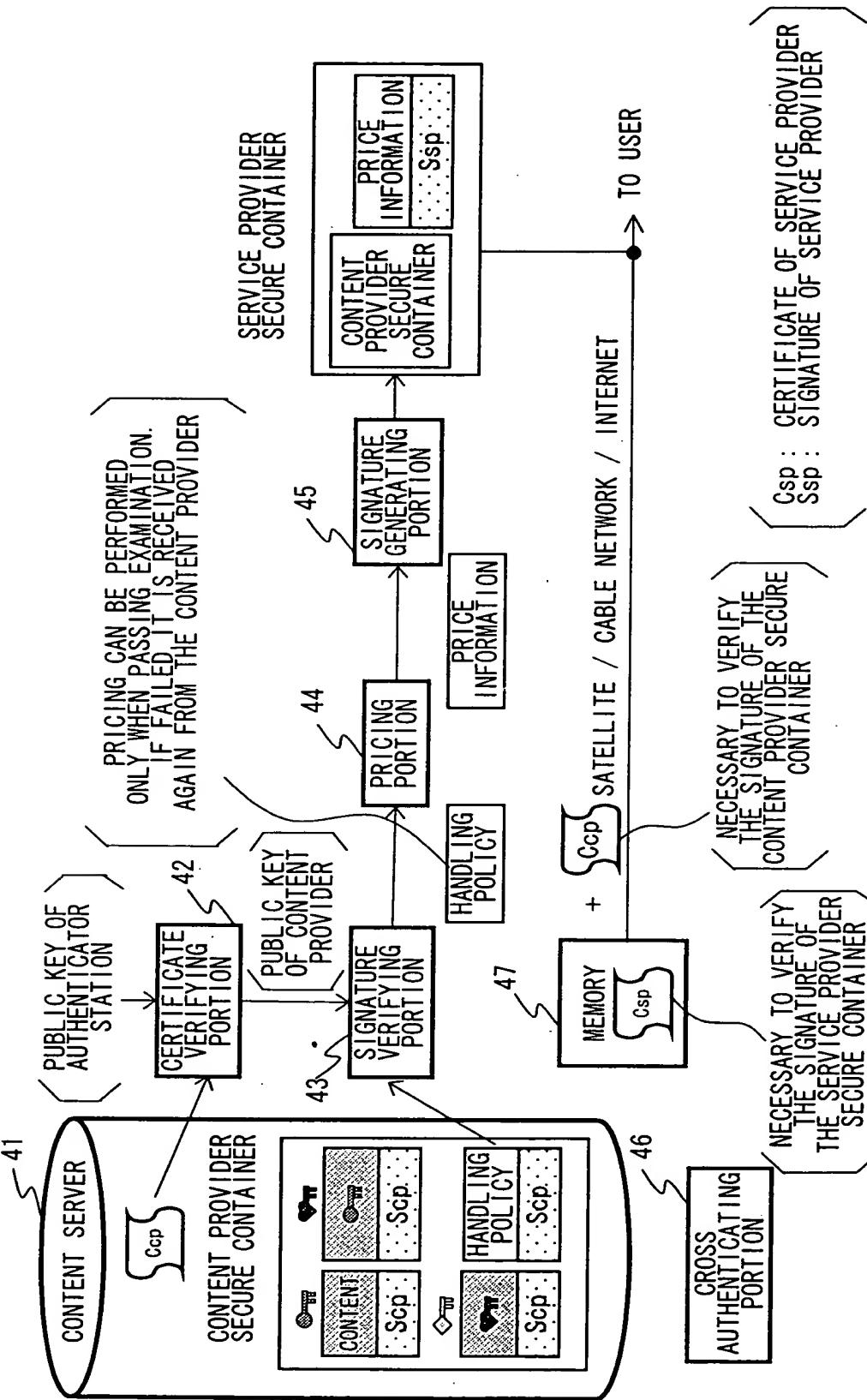
$Y_1 = Y_0/Y_v \bmod p$  IS CALCULATED

S33

A DECRYPTED TEXT  $(X_1, Y_1) = (M_x, M_y)$  IS OBTAINED

S34

FIG. 13



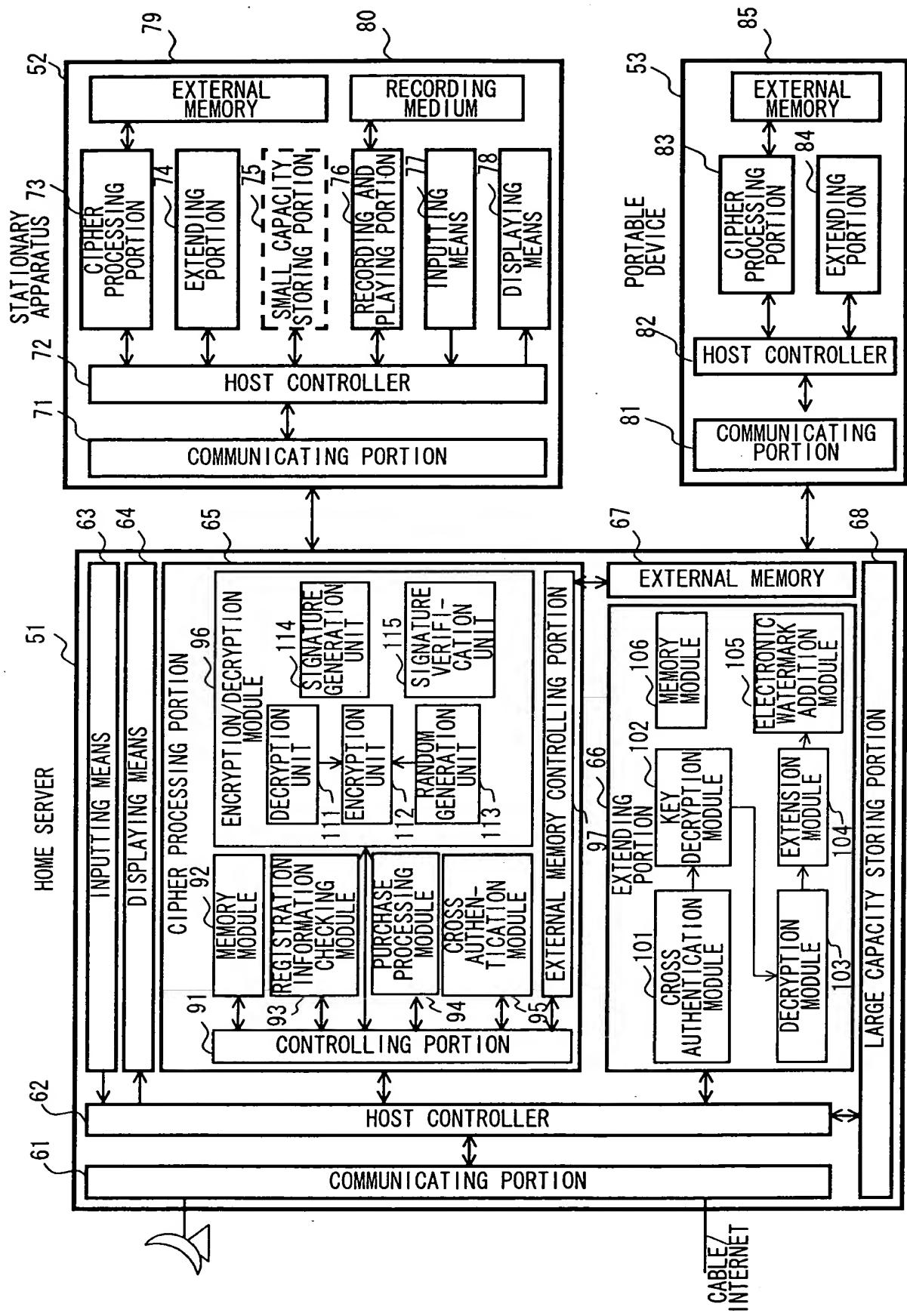


FIG. 15

09/830392

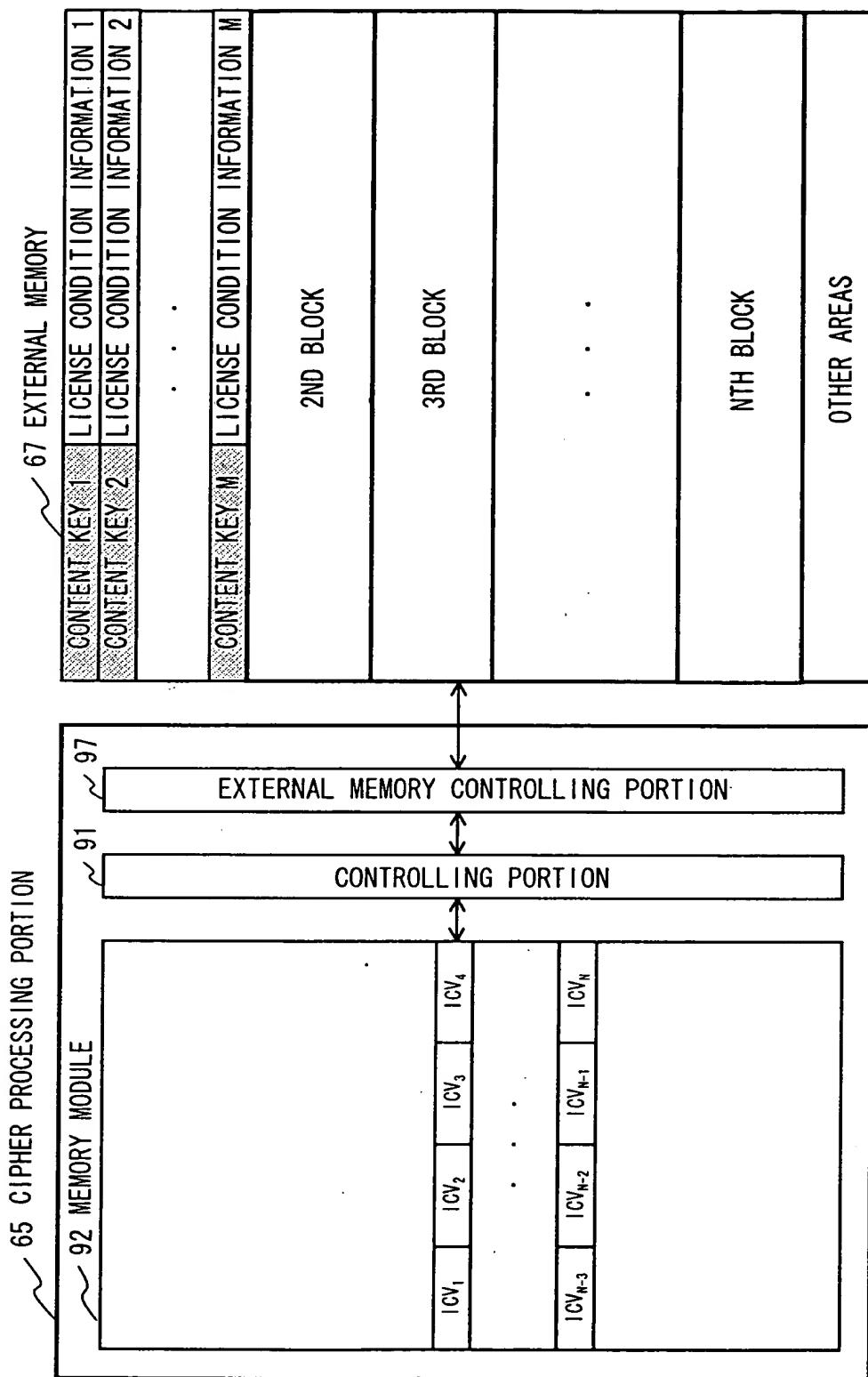


FIG. 16

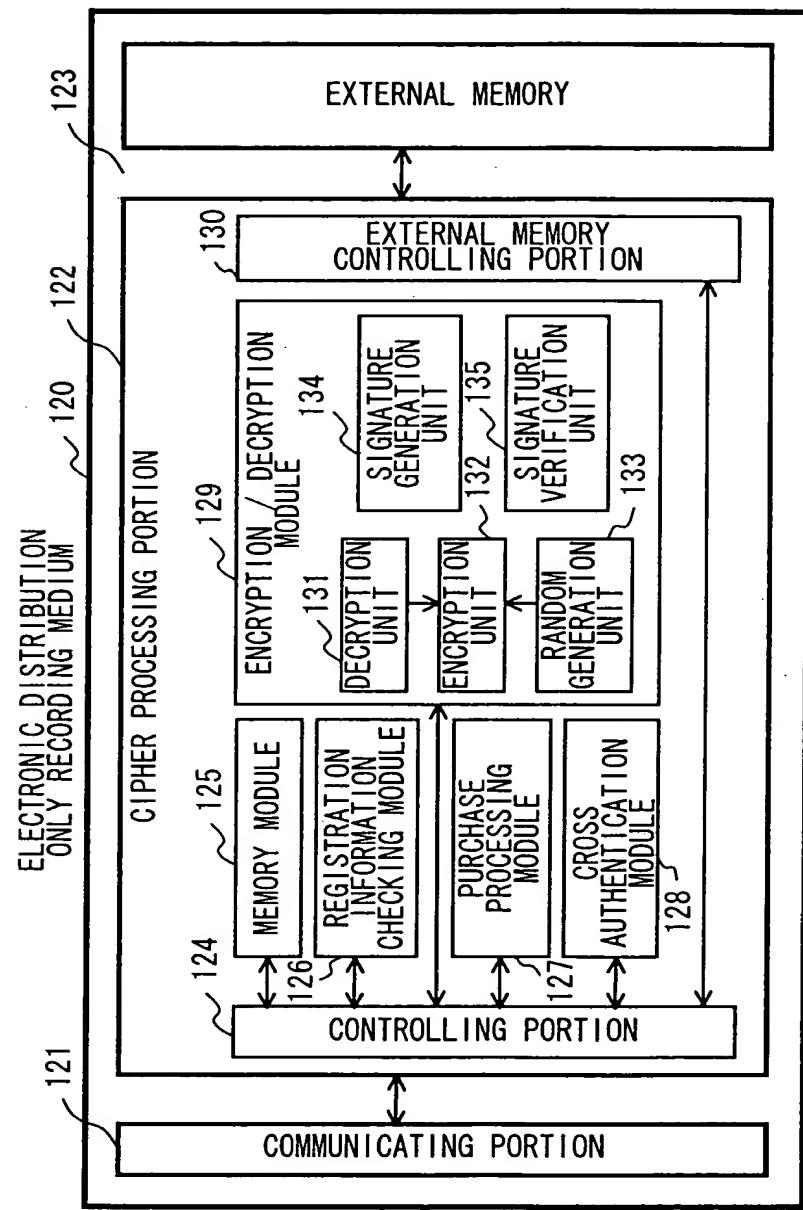


FIG. 17

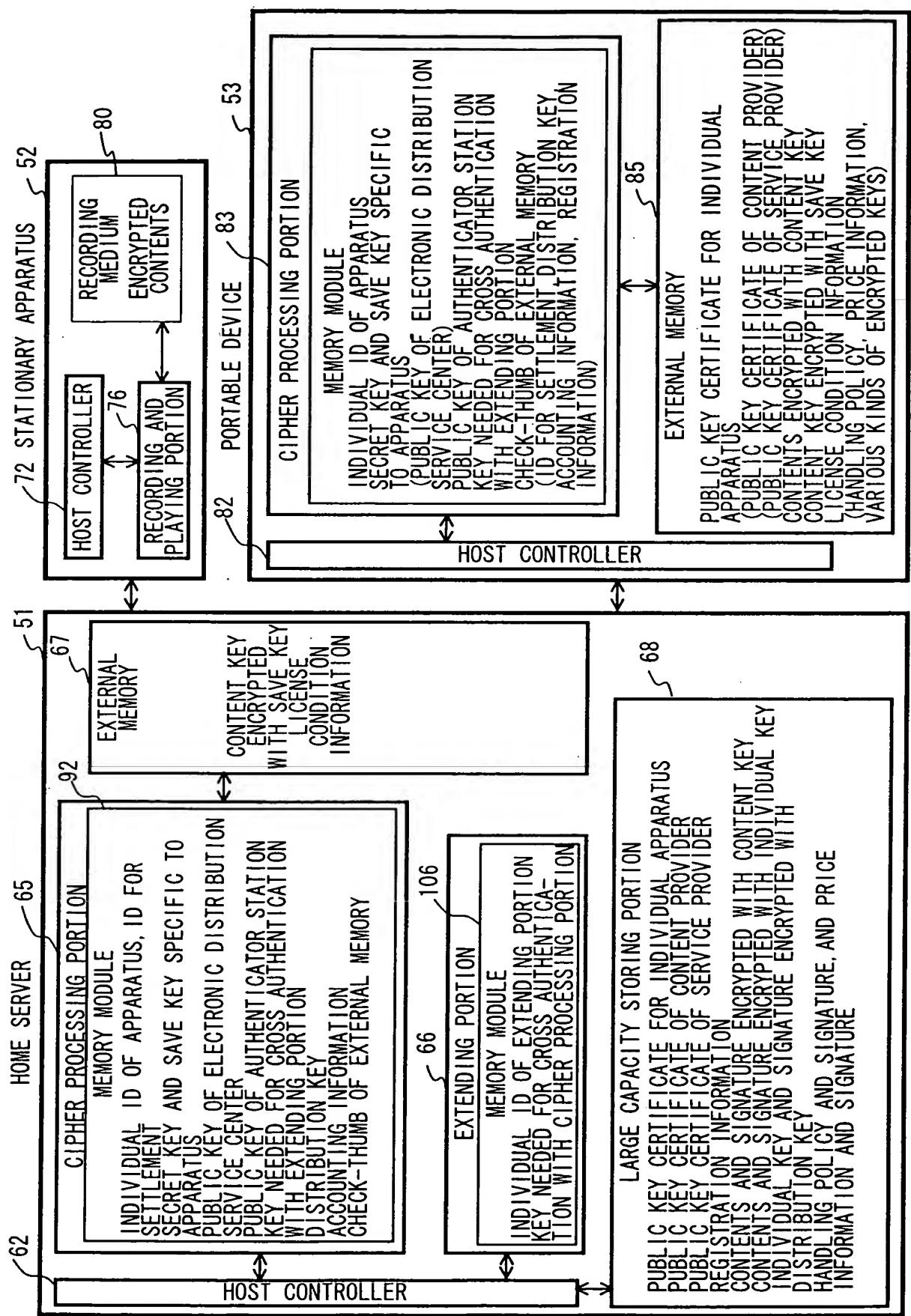


FIG. 18

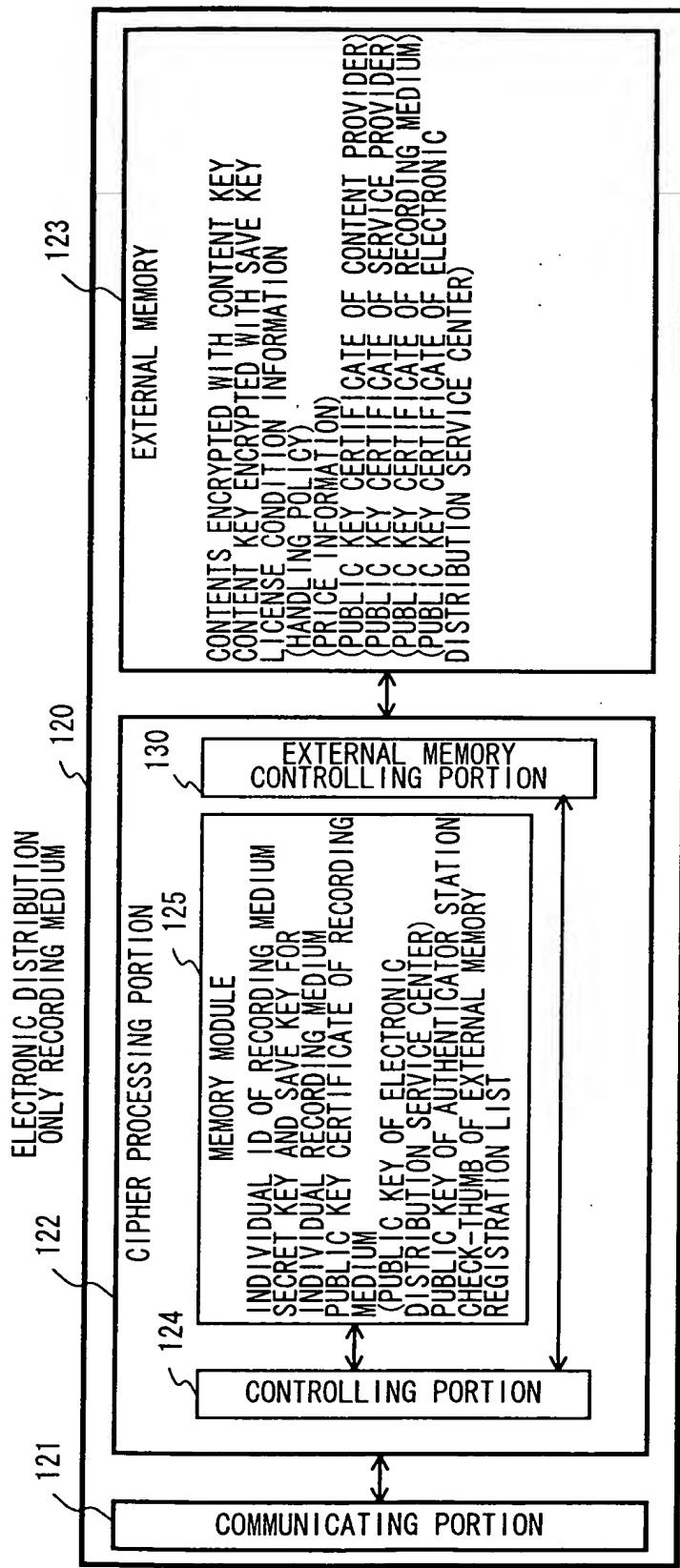


FIG. 19

09/830392

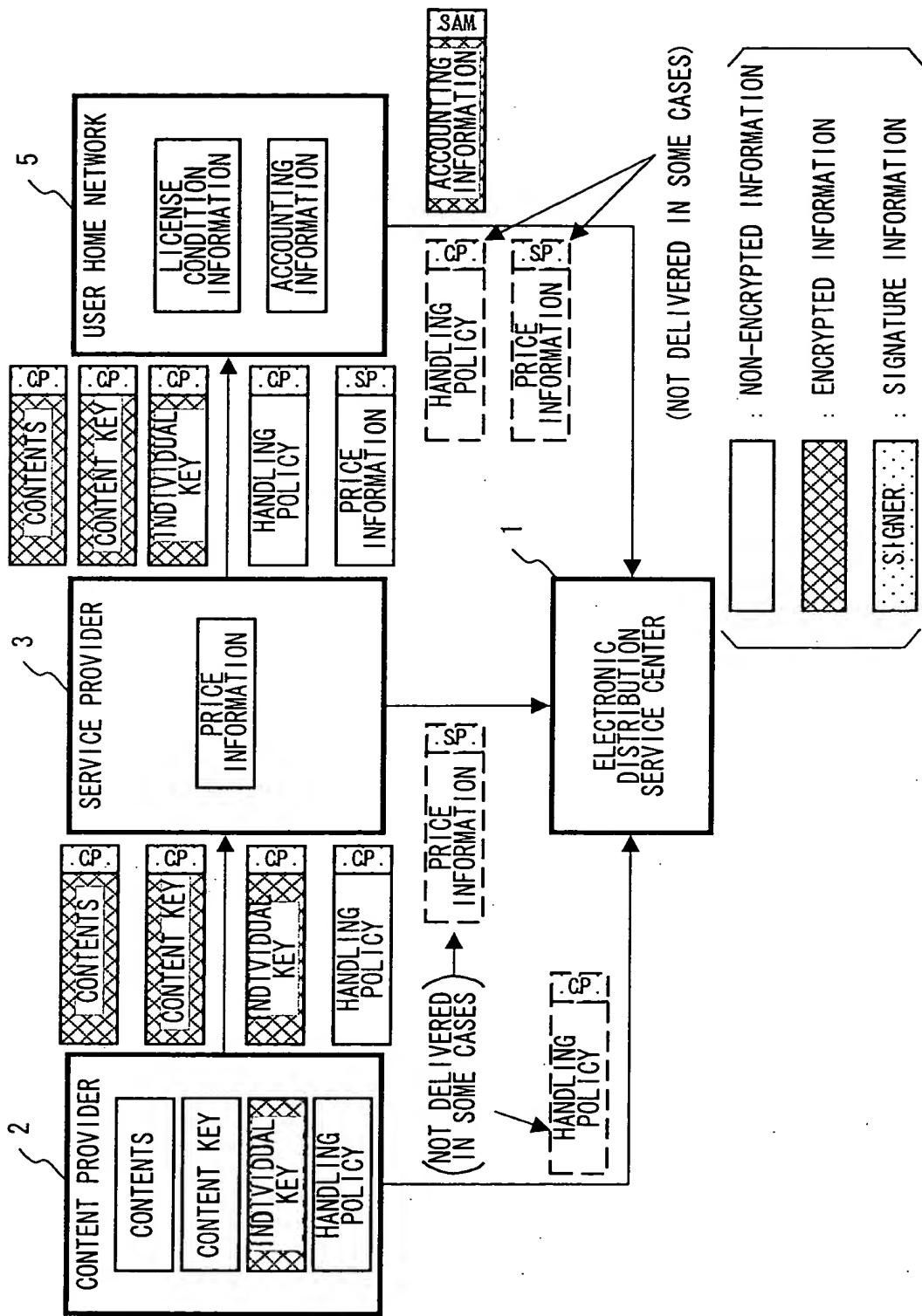


FIG. 20

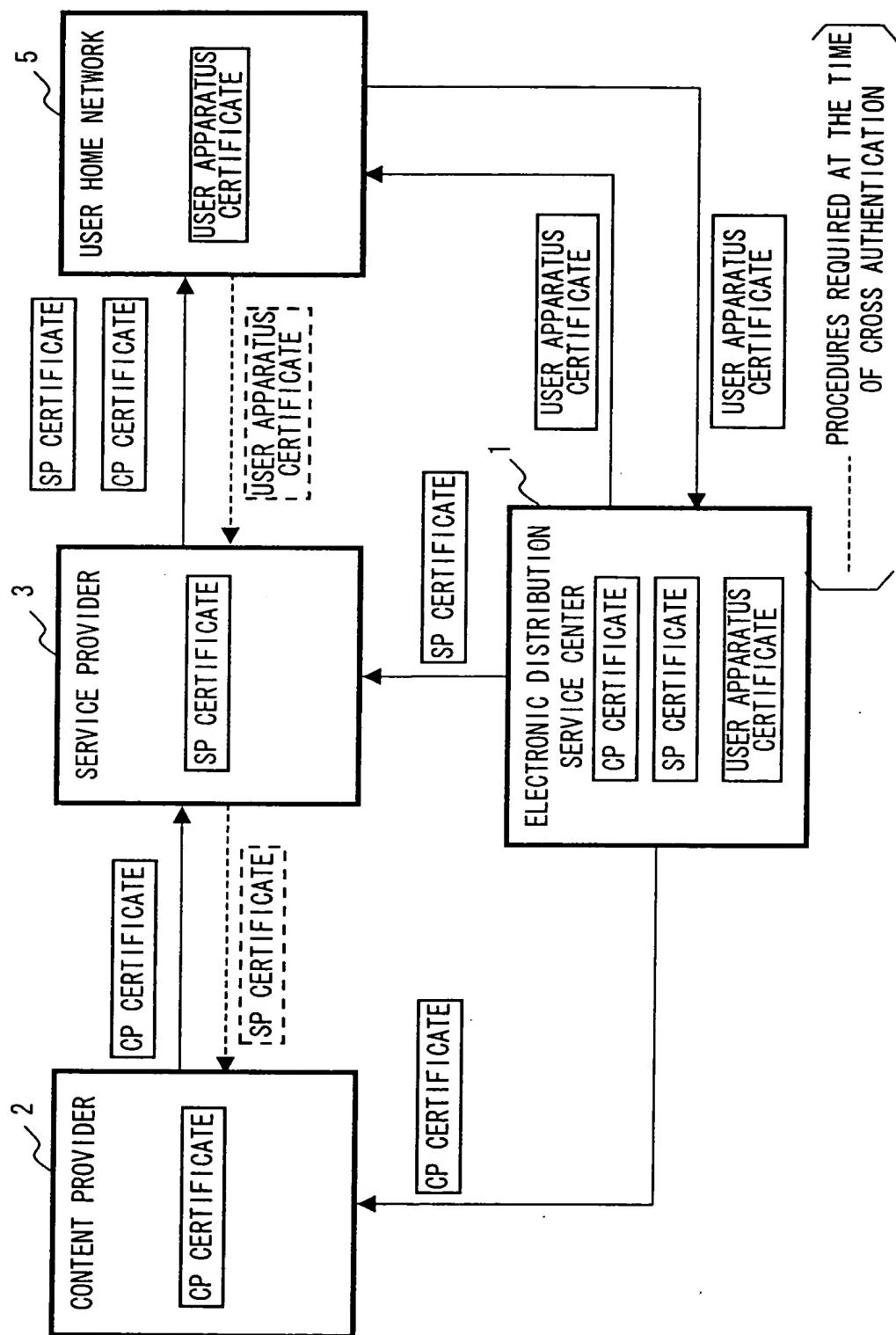


FIG. 21

09/830392

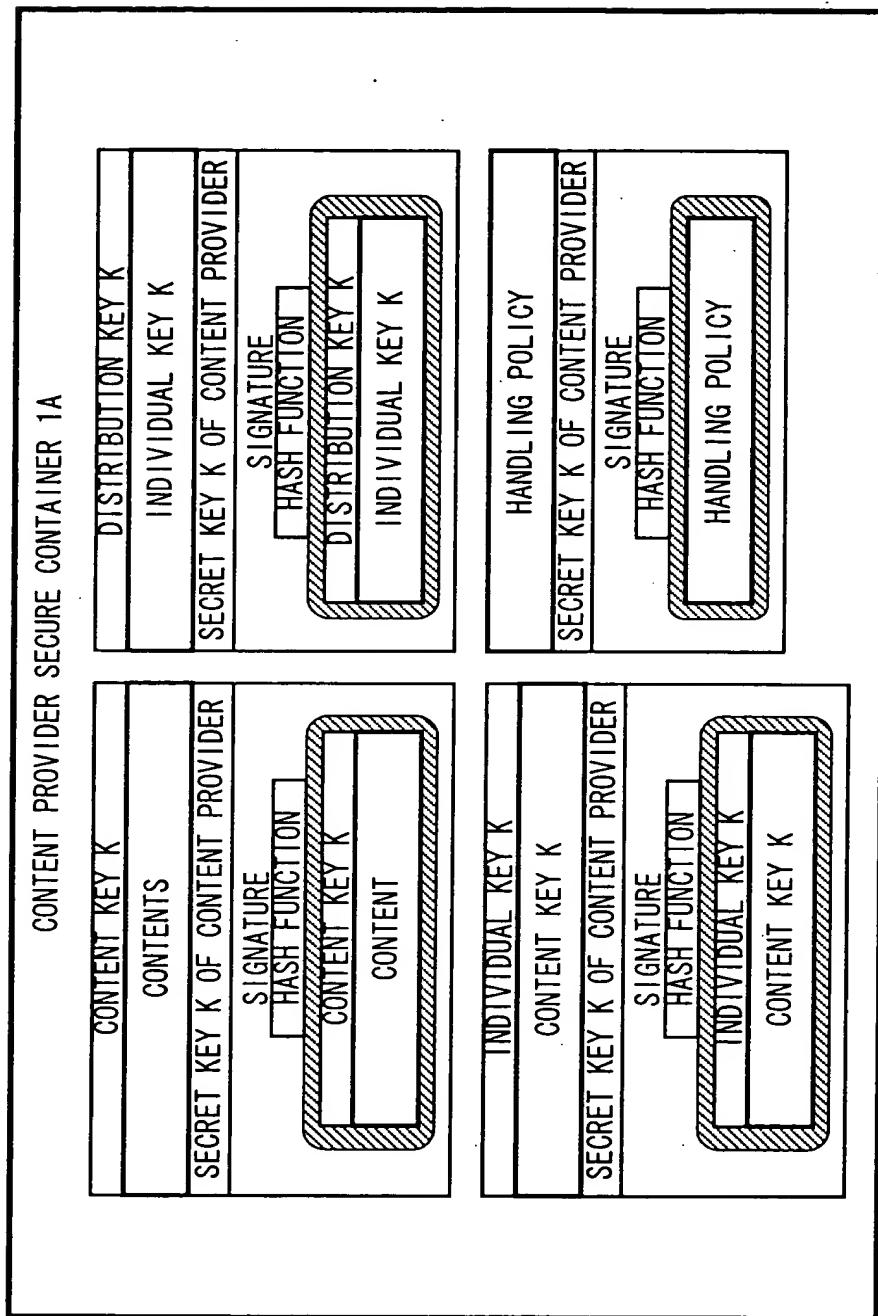


FIG. 22

09/830392

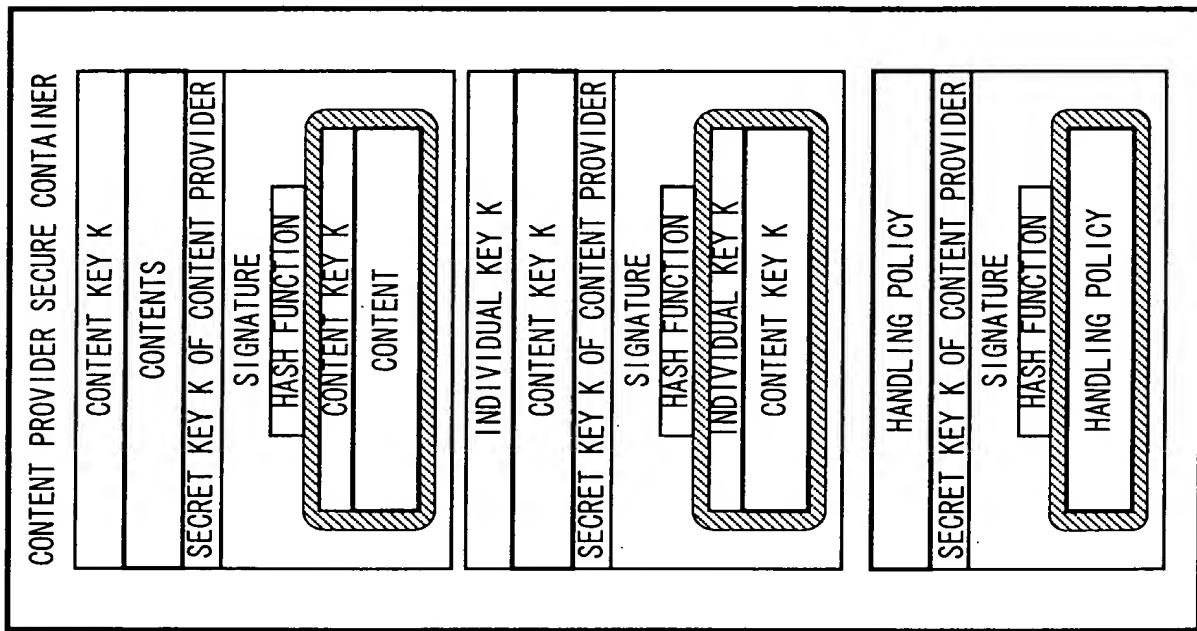


FIG. 23

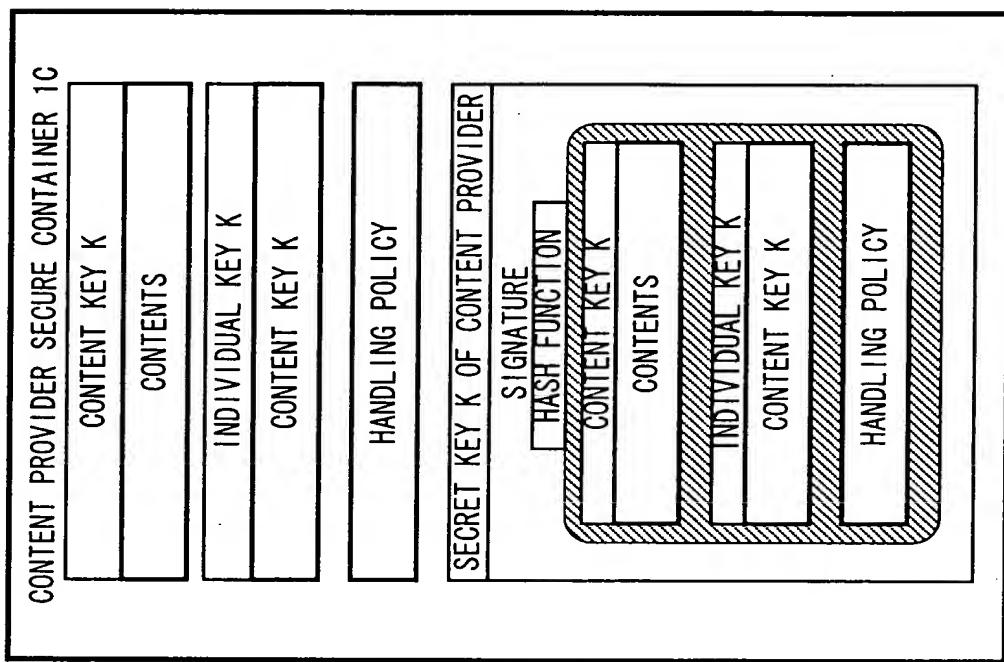


FIG. 24

09/830392

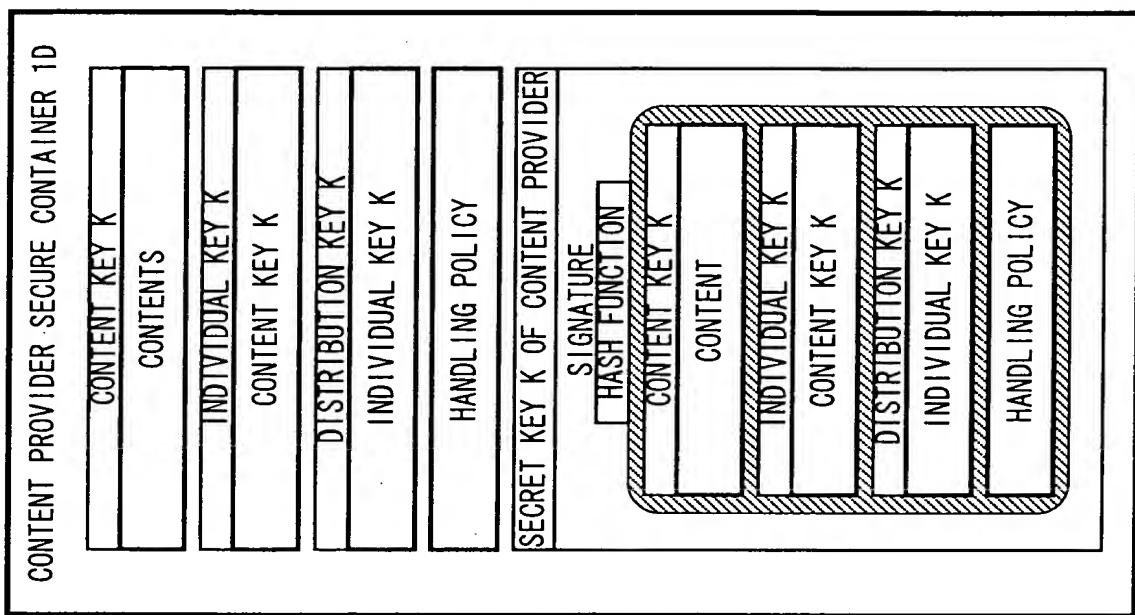


FIG. 25

09/830392

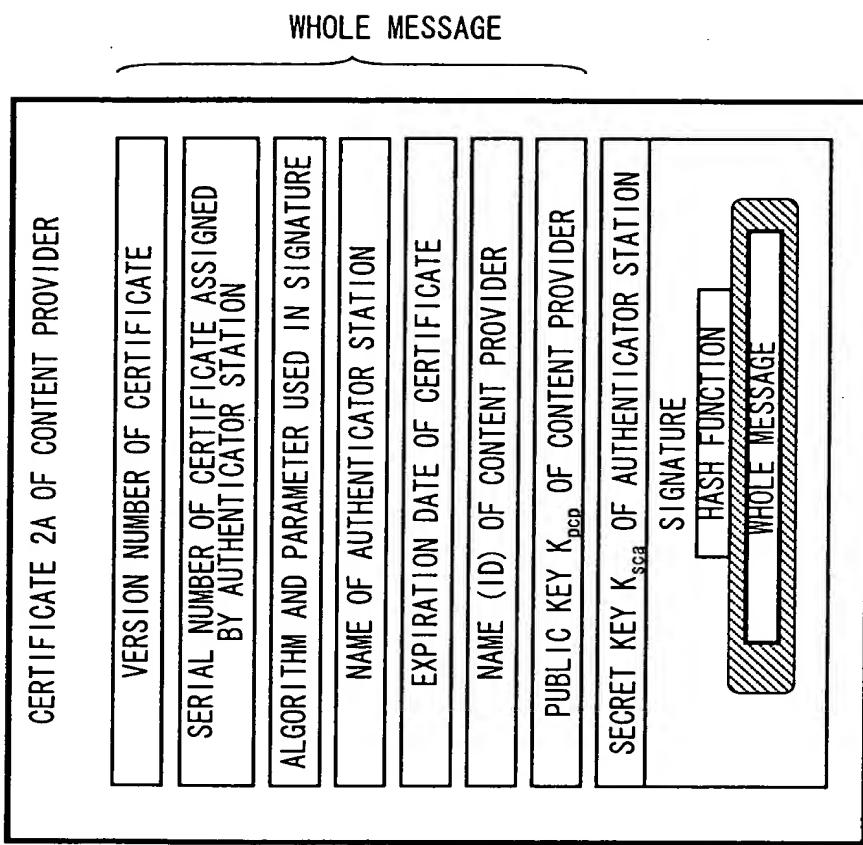


FIG. 26

09/830392

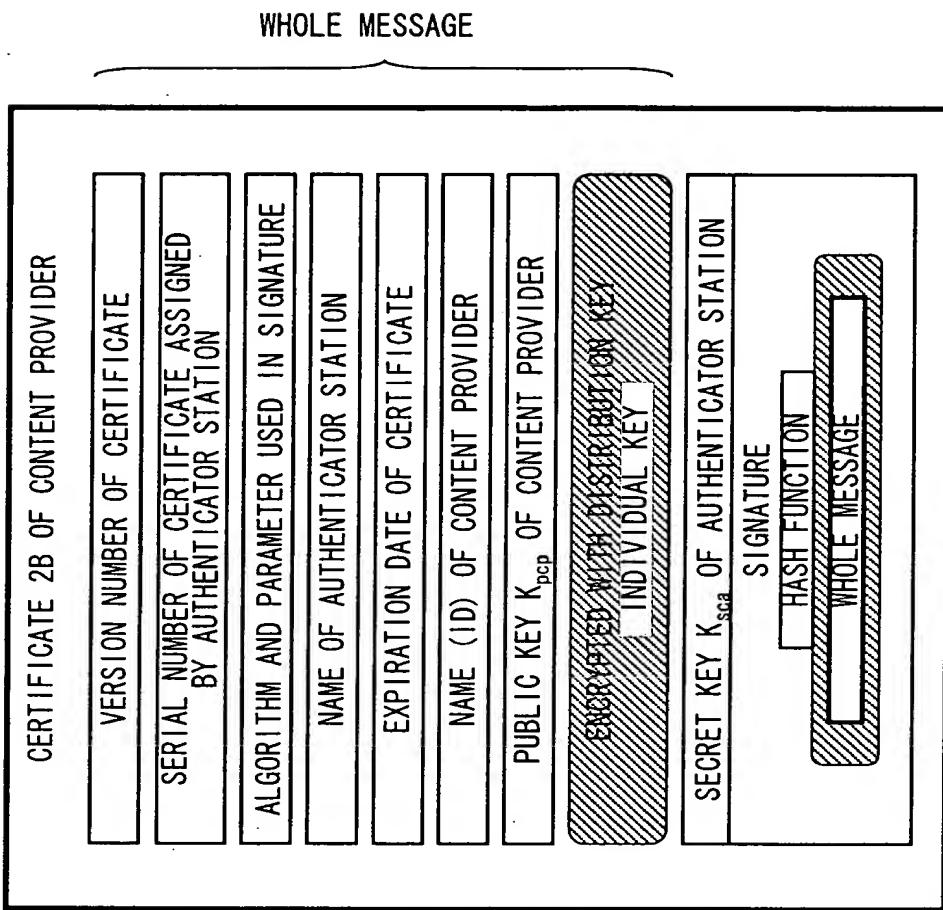


FIG. 27

09/830392

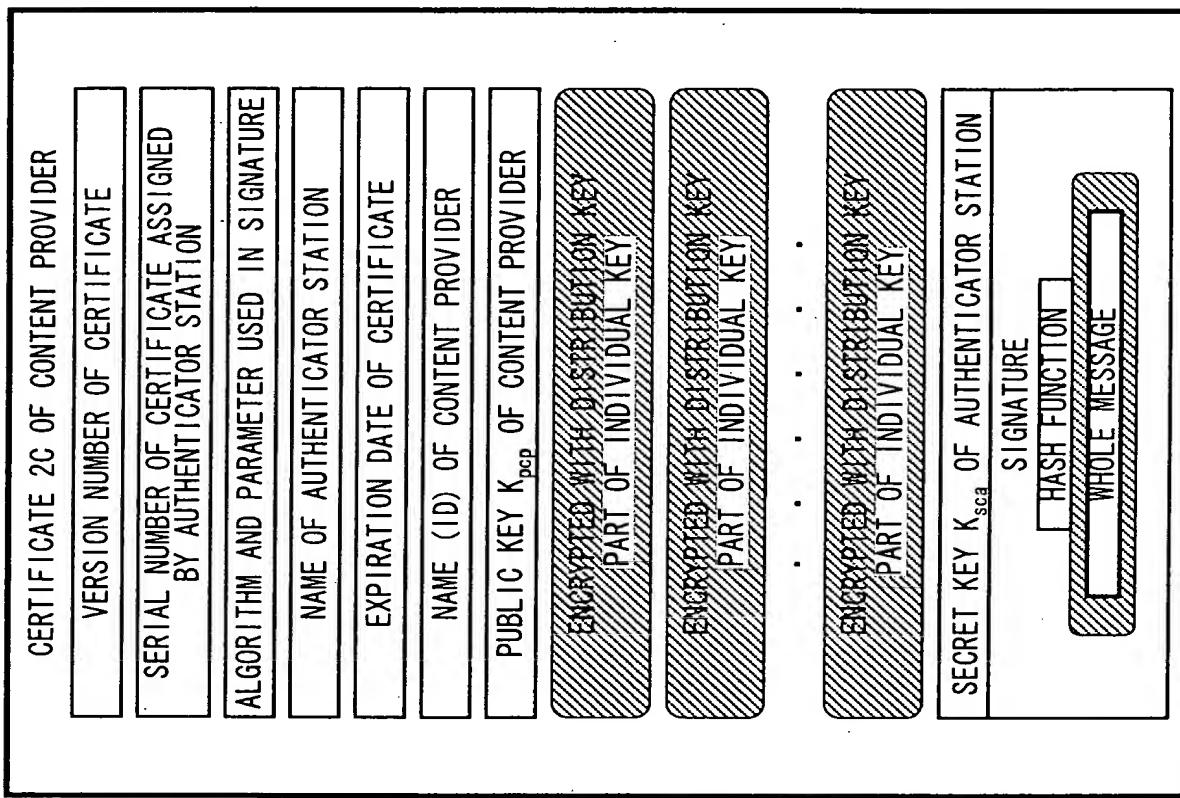
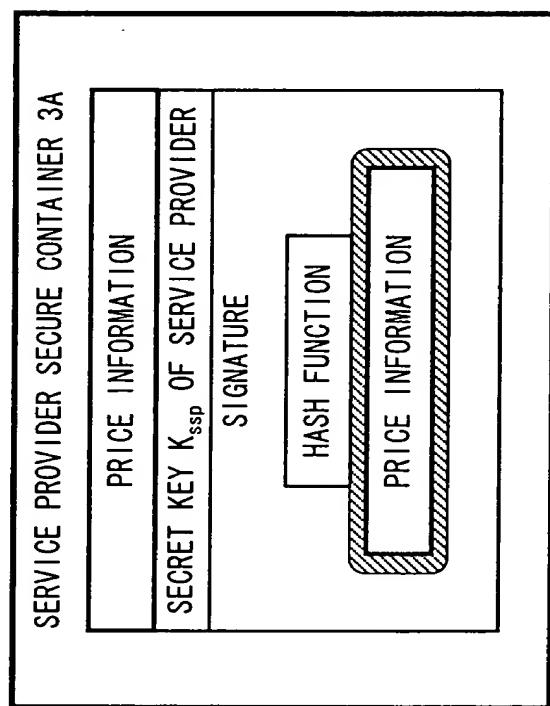


FIG. 28



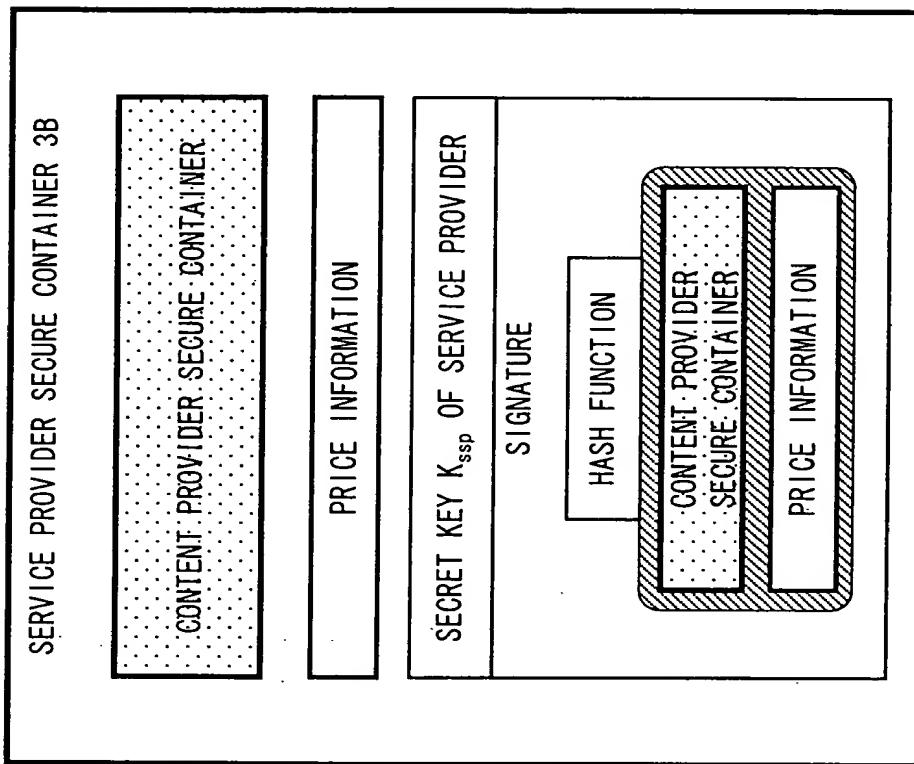


FIG. 30

09/830392

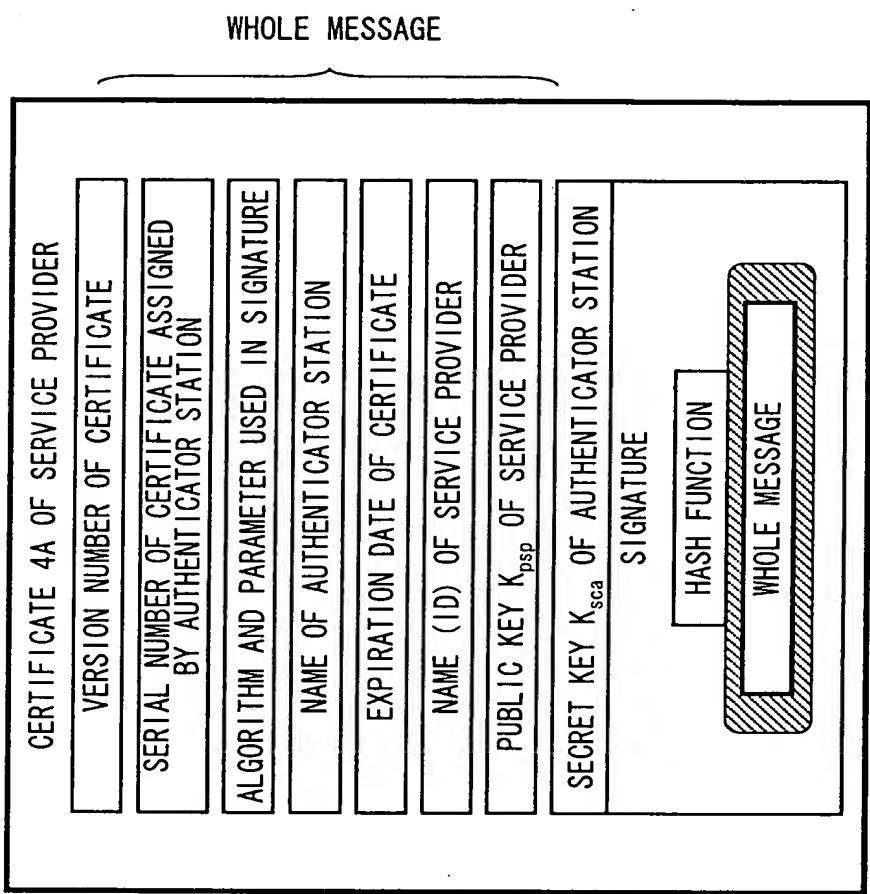


FIG. 31

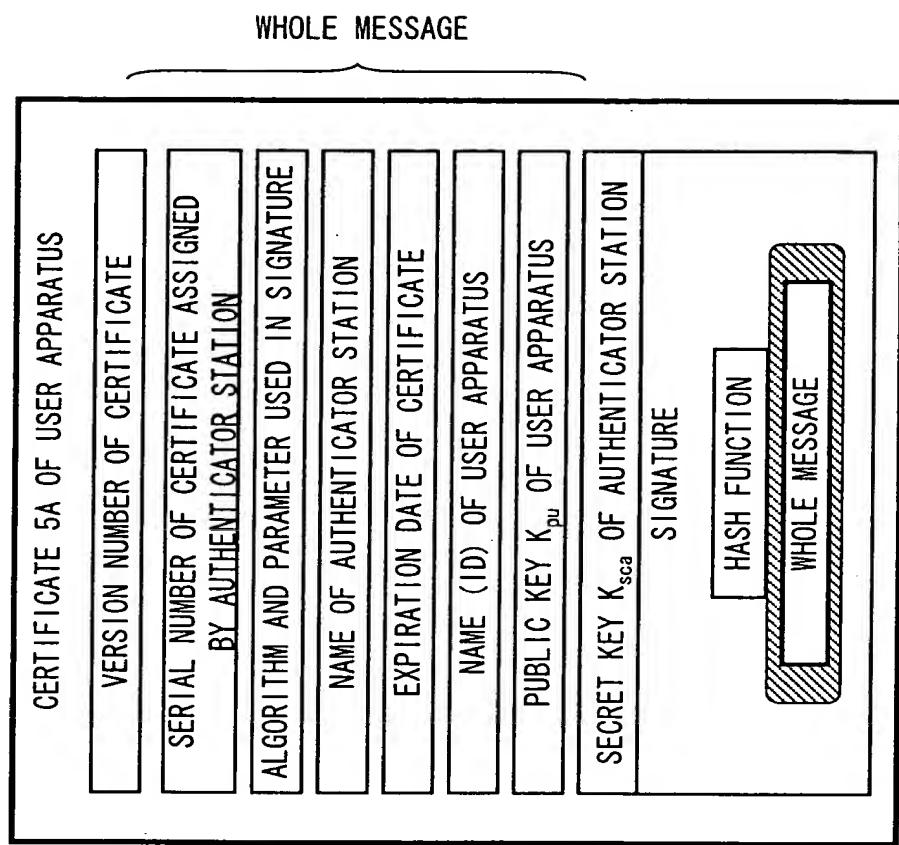


FIG. 32

TYPE OF DATA	
TYPE OF HANDLING POLICY (SINGLE)	
EXPIRATION DATE OF HANDLING POLICY	
ID OF CONTENTS	
ID OF CONTENT PROVIDER	
ID OF HANDLING POLICY	
VERSION OF HANDLING POLICY	
AREA CODE	
USAGE POSSIBLE APPARATUS CONDITION	
USAGE POSSIBLE USER CONDITION	
ID OF SERVICE PROVIDER	
GENERATION MANAGEMENT INFORMATION	
THE NUMBER OF RULES	
ADDRESS INFORMATION OF RULES	
RULE 1	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
	MINIMUM SELLING-PRICE
	AMOUNT OF BENEFITS OF CONTENT PROVIDER
	RATE OF BENEFITS OF SERVICE PROVIDER
	DATA SIZE
RULE N	SENDING INFORMATION
	•
	•
	•
	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
MINIMUM SELLING-PRICE	
AMOUNT OF BENEFITS OF CONTENT PROVIDER	
RATE OF BENEFITS OF SERVICE PROVIDER	
DATA SIZE	
SENDING INFORMATION	
(PRESENCE OR ABSENCE OF VERIFICATION OF SIGNATURE)	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 33

TYPE OF DATA	
TYPE OF HANDLING POLICY (ALBUM)	
EXPIRATION DATE OF HANDLING POLICY	
ID OF ALBUM	
VERSION OF HANDLING POLICY	
ID OF CONTENT PROVIDER	
ID OF HANDLING POLICY	
AREA CODE	
USAGE POSSIBLE APPARATUS CONDITION	
USAGE POSSIBLE USER CONDITION	
ID OF SERVICE PROVIDER	
NUMBER OF HANDLING POLICIES OF SINGLE CONTENTS	
ADDRESS INFORMATION OF HANDLING POLICY OF SINGLE CONTENTS	
SINGLE	HANDLING POLICY 1
	•
	•
	•
	HANDLING POLICY N
GENERATION MANAGEMENT INFORMATION	
NUMBER OF RULES	
ADDRESS INFORMATION OF RULES	
RULE 1	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
	MINIMUM SELLING-PRICE
	AMOUNT OF BENEFITS OF CONTENT PROVIDER
	RATE OF BENEFITS OF SERVICE PROVIDER
	DATA SIZE
RULE N	SENDING INFORMATION
	•
	•
	•
	•
	•
	•
RULE NUMBER (RULE #)	
USAGE RIGHT CONTENT NUMBER (TYPE)	
PARAMETER	
MINIMUM SELLING-PRICE	
AMOUNT OF BENEFITS OF CONTENT PROVIDER	
RATE OF BENEFITS OF SERVICE PROVIDER	
DATA SIZE	
SENDING INFORMATION	
(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 34

	TYPE OF DATA
	TYPE OF HANDLING POLICY (SINGLE)
	EXPIRATION DATE OF HANDLING POLICY
	ID OF CONTENTS
	ID OF CONTENT PROVIDER
	ID OF HANDLING POLICY
	VERSION OF HANDLING POLICY
	AREA CODE
	USAGE POSSIBLE APPARATUS CONDITION
	USAGE POSSIBLE USER CONDITION
	ID OF SERVICE PROVIDER
	GENERATION MANAGEMENT INFORMATION
	THE NUMBER OF RULES
	ADDRESS INFORMATION OF RULES
RULE 1	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
	MINIMUM SELLING-PRICE
	DATA SIZE
	SENDING INFORMATION
•	•
	•
RULE N	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
	MINIMUM SELLING-PRICE
	DATA SIZE
	SENDING INFORMATION
	(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)
	PUBLIC KEY CERTIFICATE
	SIGNATURE

FIG. 35

TYPE OF DATA	
TYPE OF HANDLING POLICY (ALBUM)	
EXPIRATION DATE OF HANDLING POLICY	
ID OF ALBUM	
VERSION OF HANDLING POLICY	
ID OF CONTENT PROVIDER	
ID OF HANDLING POLICY	
AREA CODE	
USAGE POSSIBLE APPARATUS CONDITION	
USAGE POSSIBLE USER CONDITION	
ID OF SERVICE PROVIDER	
NUMBER OF HANDLING POLICIES OF SINGLE CONTENTS	
ADDRESS INFORMATION OF HANDLING POLICY OF SINGLE CONTENTS	
SINGLE	HANDLING POLICY 1
	•
	•
	HANDLING POLICY N
GENERATION MANAGEMENT INFORMATION	
NUMBER OF RULES	
ADDRESS INFORMATION OF RULES	
RULE 1	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
	MINIMUM SELLING-PRICE
	DATA SIZE
	SENDING INFORMATION
•	•
•	•
•	•
RULE N	RULE NUMBER (RULE #)
	USAGE RIGHT CONTENT NUMBER (TYPE)
	PARAMETER
	MINIMUM SELLING-PRICE
	DATA SIZE
	SENDING INFORMATION
(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 36

TYPE OF DATA	
TYPE OF PRICE INFORMATION (SINGLE)	
EXPIRATION DATE OF PRICE INFORMATION	
ID OF CONTENTS	
ID OF SERVICE PROVIDER	
ID OF PRICE INFORMATION	
VERSION OF PRICE INFORMATION	
AREA CODE	
USAGE POSSIBLE APPARATUS CONDITION	
USAGE POSSIBLE USER CONDITION	
ID OF CONTENT PROVIDER	
ID OF HANDLING POLICY	
NUMBER OF RULES	
ADDRESS INFORMATION OF RULES	
RULE 1	RULE NUMBER (RULE#)
	AMOUNT OF BENEFITS OF SERVICE PROVIDER
	RATE OF BENEFITS OF SERVICE PROVIDER
	PRICE
	DATA SIZE
	SENDING INFORMATION
RULE N	• • •
	• • •
	RULE NUMBER (RULE#)
	AMOUNT OF BENEFITS OF SERVICE PROVIDER
	RATE OF BENEFITS OF SERVICE PROVIDER
	PRICE
DATA SIZE	
SENDING INFORMATION	
(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 37

TYPE OF DATA	
TYPE OF PRICE INFORMATION (ALBUM)	
EXPIRATION DATE OF PRICE INFORMATION	
ID OF ALBUM	
ID OF SERVICE PROVIDER	
ID OF PRICE INFORMATION	
VERSION OF PRICE INFORMATION	
AREA CODE	
USAGE POSSIBLE APPARATUS CONDITION	
USAGE POSSIBLE USER CONDITION	
ID OF CONTENT PROVIDER	
ID OF HANDLING POLICY	
NUMBER OF PRICE INFORMATION OF SINGLE CONTENTS	
ADDRESS INFORMATION OF PRICE INFORMATION OF SINGLE CONTENTS	
SINGLE	PRICE INFORMATION 1
	⋮
PRICE INFORMATION N	
NUMBER OF RULES	
ADDRESS INFORMATION OF RULES	
RULE 1	RULE NUMBER (RULE#)
	AMOUNT OF BENEFITS OF SERVICE PROVIDER
	RATE OF BENEFITS OF SERVICE PROVIDER
	PRICE
	DATA SIZE
	SENDING INFORMATION
⋮	⋮
RULE N	RULE NUMBER (RULE#)
	AMOUNT OF BENEFITS OF SERVICE PROVIDER
	RATE OF BENEFITS OF SERVICE PROVIDER
	PRICE
	DATA SIZE
	SENDING INFORMATION
(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 38

TYPE OF DATA	
TYPE OF PRICE INFORMATION (SINGLE)	
EXPIRATION DATE OF PRICE INFORMATION	
ID OF CONTENTS	
ID OF SERVICE PROVIDER	
ID OF PRICE INFORMATION	
VERSION OF PRICE INFORMATION	
AREA CODE	
USAGE POSSIBLE APPARATUS CONDITION	
USAGE POSSIBLE USER CONDITION	
ID OF CONTENT PROVIDER	
ID OF HANDLING POLICY	
NUMBER OF RULES	
ADDRESS INFORMATION OF RULES	
RULE 1	RULE NUMBER (RULE#)
	PRICE
	DATA SIZE
	SENDING INFORMATION
•	•
	•
RULE N	RULE NUMBER (RULE#)
	PRICE
	DATA SIZE
	SENDING INFORMATION
	(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 39

TYPE OF DATA	
TYPE OF PRICE INFORMATION (ALBUM)	
EXPIRATION DATE OF PRICE INFORMATION	
ID OF ALBUM	
ID OF SERVICE PROVIDER	
ID OF PRICE INFORMATION	
VERSION OF PRICE INFORMATION	
AREA CODE	
USAGE POSSIBLE APPARATUS CONDITION	
USAGE POSSIBLE USER CONDITION	
ID OF CONTENT PROVIDER	
ID OF HANDLING POLICY	
NUMBER OF PRICE INFORMATION OF SINGLE CONTENTS	
ADDRESS INFORMATION OF PRICE INFORMATION OF SINGLE CONTENTS	
SINGLE	PRICE INFORMATION 1
	• •
PRICE INFORMATION N	
NUMBER OF RULES	
ADDRESS INFORMATION OF RULES	
RULE 1	RULE NUMBER (RULE#)
	PRICE
	DATA SIZE
	SENDING INFORMATION
• •	• •
RULE N	RULE NUMBER (RULE#)
	PRICE
	DATA SIZE
	SENDING INFORMATION
(PRESENCE OR ABSENCE OF DETECTION OF SIGNATURE)	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 40

TYPE OF DATA
TYPE OF LICENSE CONDITION INFORMATION
EXPIRATION DATE OF LICENSE CONDITION INFORMATION
ID OF CONTENTS
ID OF ALBUM
ID OF CIPHER PROCESSING PORTION
ID OF USER
ID OF CONTENT PROVIDER
ID OF HANDLING POLICY
VERSION OF HANDLING POLICY
ID OF SERVICE PROVIDER
ID OF PRICE INFORMATION
VERSION OF PRICE INFORMATION
ID OF LICENSE CONDITION INFORMATION
RULE NUMBER OF PLAYBACK RIGHT (USAGE RIGHT)
USAGE RIGHT CONTENT NUMBER
REMAINING NUMBER OF TIMES OF PLAYBACK
EXPIRATION DATE OF PLAYBACK RIGHT
RULE NUMBER OF REPLICATION RIGHT (USAGE RIGHT)
USAGE RIGHT CONTENT NUMBER
REMAINING NUMBER OF TIMES OF REPLICATION
GENERATION MANAGEMENT INFORMATION
ID OF CIPHER PROCESSING PORTION POSSESSING PLAYBACK RIGHT

TOP SECRET//~~REF ID: A65660~~

FIG. 41

TYPE OF DATA
ID OF CIPHER PROCESSING PORTION
ID OF USER
ID OF CONTENTS
ID OF CONTENT PROVIDER
ID OF HANDLING POLICY
VERSION OF HANDLING POLICY
ID OF SERVICE PROVIDER
ID OF PRICE INFORMATION
VERSION OF PRICE INFORMATION
ID OF LICENSE CONDITION INFORMATION
RULE NUMBER (RULE #)
AMOUNT / RATE OF BENEFITS OF CONTENT PROVIDER
AMOUNT / RATE OF BENEFITS OF SERVICE PROVIDER
GENERATION MANAGEMENT INFORMATION
DATA SIZE OF SENDING INFORMATION DEFINED BY CONTENT PROVIDER
SENDING INFORMATION DEFINED BY CONTENT PROVIDER
DATA SIZE OF SENDING INFORMATION DEFINED BY SERVICE PROVIDER
SENDING INFORMATION DEFINED BY SERVICE PROVIDER
ID OF SUPPLIER

FIG. 42

TYPE OF DATA
ID OF CIPHER PROCESSING PORTION
ID OF USER
ID OF CONTENTS
ID OF CONTENT PROVIDER
ID OF HANDLING POLICY
VERSION OF HANDLING POLICY
ID OF SERVICE PROVIDER
ID OF PRICE INFORMATION
VERSION OF PRICE INFORMATION
ID OF LICENSE CONDITION INFORMATION
RULE NUMBER (RULE #)
GENERATION MANAGEMENT INFORMATION
DATA SIZE OF SENDING INFORMATION DEFINED BY CONTENT PROVIDER
SENDING INFORMATION DEFINED BY CONTENT PROVIDER
DATA SIZE OF SENDING INFORMATION DEFINED BY SERVICE PROVIDER
SENDING INFORMATION DEFINED BY SERVICE PROVIDER
ID OF SUPPLIER

FIG. 43

USAGE RIGHT CONTENT NUMBER	RIGHT	USAGE RIGHT CONTENT		
		LIMIT ON PERIOD	NUMBER OF TIMES	LIMIT ON REPLICATION
(1)	NOT IMPOSED	NOT IMPOSED	—	—
(2)	IMPOSED	NOT IMPOSED	—	—
(3)	IMPOSED	NOT IMPOSED	—	—
(4)	NOT IMPOSED	IMPOSED	—	—
(5)	NOT IMPOSED	NOT IMPOSED	NOT IMPOSED	NOT IMPOSED
(6)	NOT IMPOSED	IMPOSED	NOT IMPOSED	NOT IMPOSED
(7)	NOT IMPOSED	NOT IMPOSED	NOT IMPOSED	NOT IMPOSED
(8)	NOT IMPOSED	IMPOSED	SCMS	SCMS
(9) ~ (15)	SPARES			
(16)	RIGHT TO CHANGE RIGHT CONTENTS	—		
(17)	REPURCHASE RIGHT	—		
(18)	ADDITIONAL PURCHASE RIGHT	—		
(19)	MANAGEMENT TRANSFER RIGHT	—		

FIG. 44

(A)	EXPIRATION DATE OF PLAYBACK RIGHT
(B)	EXPIRATION DATE OF PLAYBACK RIGHT
(C)	EXPIRATION DATE OF PLAYBACK RIGHT NUMBER OF DAYS AND TIME
(D)	EXPIRATION DATE OF PLAYBACK RIGHT NUMBER OF TIMES OF PLAYBACK
(E)	EXPIRATION DATE OF REPLICATION RIGHT
(F)	EXPIRATION DATE OF REPLICATION DATE NUMBER OF TIMES OF REPLICATION
(G)	EXPIRATION DATE OF REPLICATION
(H)	EXPIRATION DATE OF REPLICATION NUMBER OF TIMES OF REPLICATION
(I)	EXPIRATION DATE OF RIGHT TO CHANGE RIGHT CONTENTS FORMER RULE NUMBER NEW RULE NUMBER
(J)	EXPIRATION DATE OF REPURCHASE RIGHT FORMER RULE NUMBER NEW RULE NUMBER MAXIMUM REDISTRIBUTED GENERATION INFORMATION
(K)	EXPIRATION DATE OF ADDITIONAL PURCHASE RIGHT MINIMUM NUMBER OF POSSESSED CONTENTS MAXIMUM NUMBER OF POSSESSED CONTENTS
(L)	EXPIRATION DATE OF MANAGEMENT TRANSFER RIGHT
(M)	EXPIRATION DATE OF CONTENT PURCHASE RIGHT ID OF FORMER CONTENTS FORMER RULE NUMBER NEW RULE NUMBER

FIG. 45

TYPE OF DATA
TYPE OF CONTENTS (SINGLE)
EXPIRATION DATE OF CONTENTS
CATEGORY OF CONTENTS
ID OF CONTENTS
ID OF CONTENT PROVIDER
CRYPTOSYSTEM OF CONTENTS
DATA LENGTH OF ENCRYPTED CONTENTS
ENCRYPTED CONTENTS
PUBLIC KEY CERTIFICATE
SIGNATURE

FIG. 46

TYPE OF DATA	
TYPE OF CONTENTS (ALBUM)	
EXPIRATION DATE OF CONTENTS	
ID OF ALBUM	
ID OF CONTENT PROVIDER	
NUMBER OF SINGLE CONTENTS	
ADDRESS INFORMATION OF SINGLE CONTENTS	
SINGLE	CONTENTS 1
	• •
CONTENTS N	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 47

09/830392 " 09/830392

TYPE OF DATA
TYPE OF KEY DATA (SINGLE)
EXPIRATION DATE OF KEY
ID OF CONTENTS
ID OF CONTENT PROVIDER
KEY VERSION
CRYPTOSYSTEM OF CONTENT KEY
ENCRYPTED CONTENT KEY
CRYPTOSYSTEM OF INDIVIDUAL KEY
ENCRYPTED INDIVIDUAL KEY
PUBLIC KEY CERTIFICATE
SIGNATURE

FIG. 48

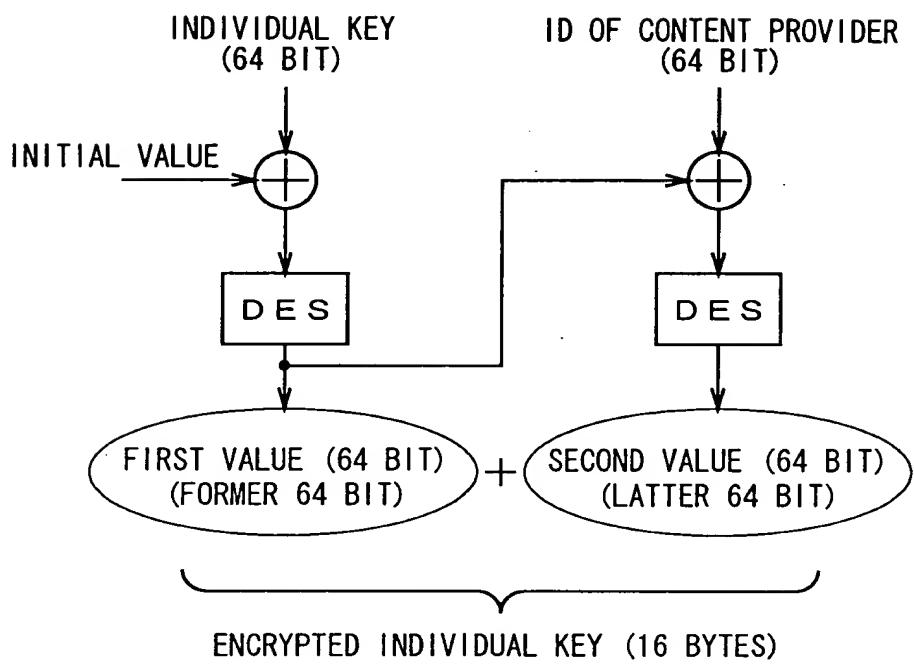


FIG. 49

09/830392

TYPE OF DATA	
TYPE OF KEY DATA (ALBUM)	
EXPIRATION DATE OF KEY	
ID OF ALBUM	
CONTENT PROVIDER ID	
VERSION OF KEY	
NUMBER OF KEY DATA FOR SINGLE CONTENTS	
ADDRESS INFORMATION OF KEY DATA FOR SINGLE CONTENTS	
SINGLE	KEY DATA 1
	• •
KEY DATA N	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

FIG. 50

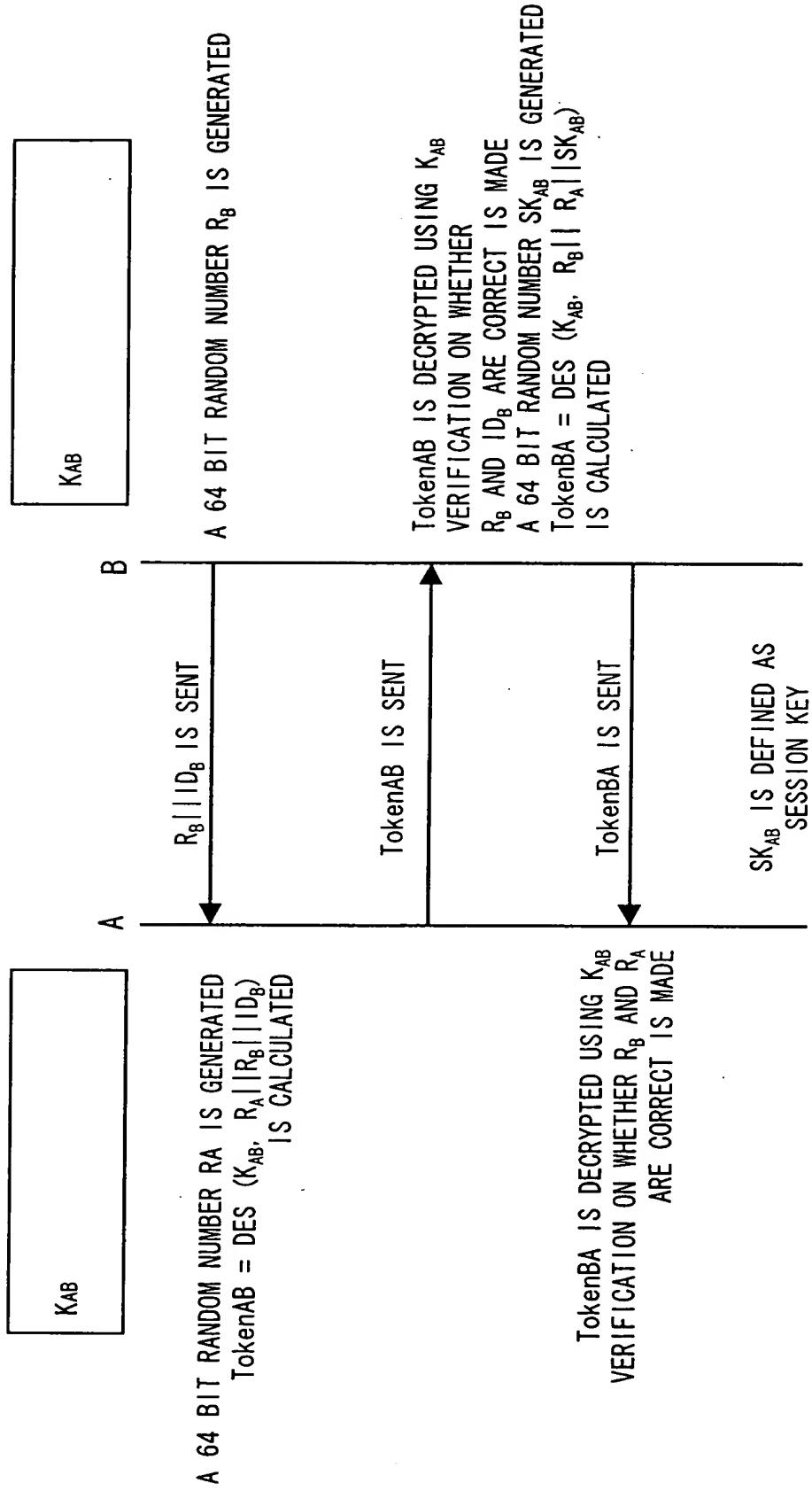
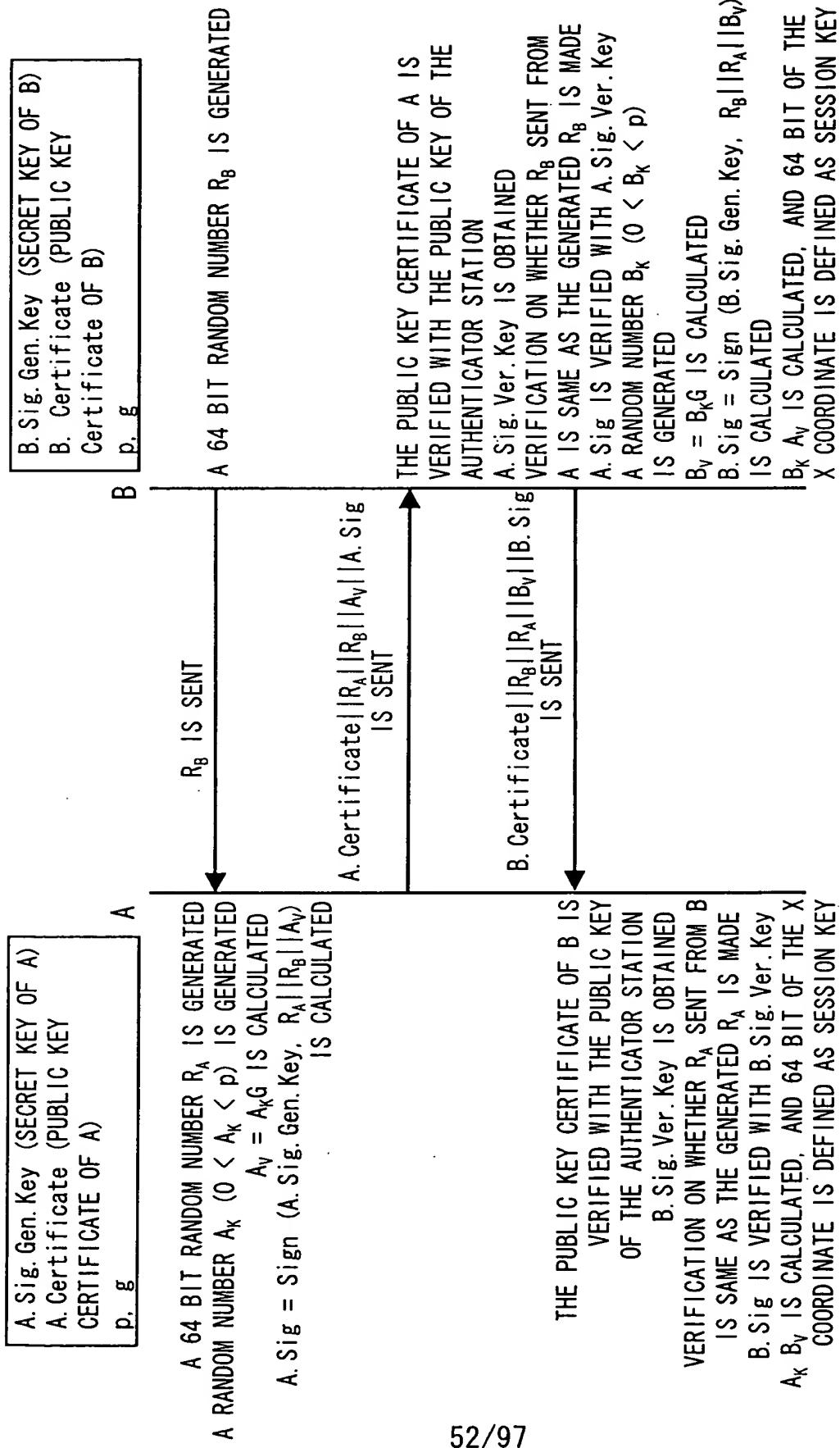


FIG. 51



(DATA WITH SIGNATURE)

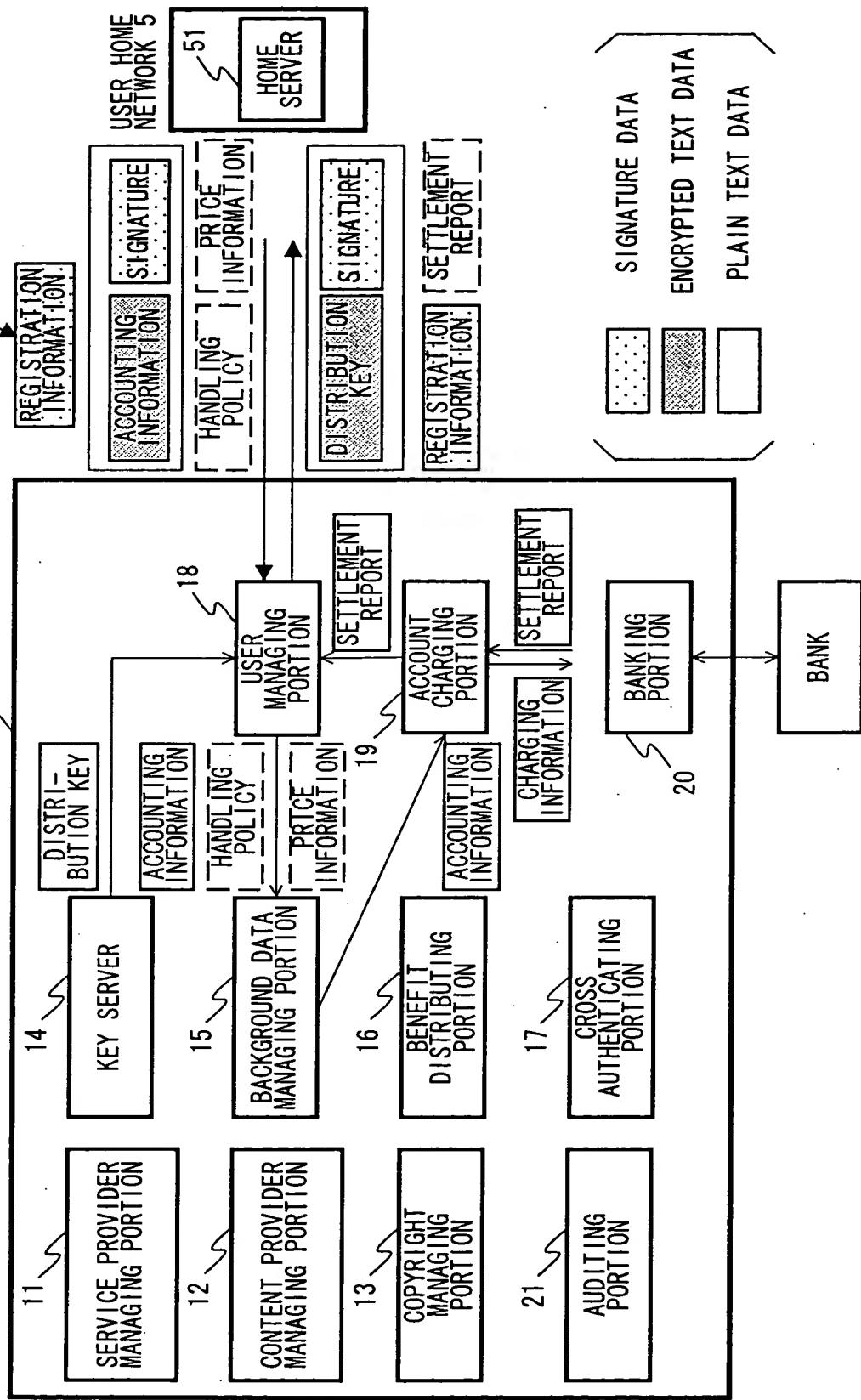
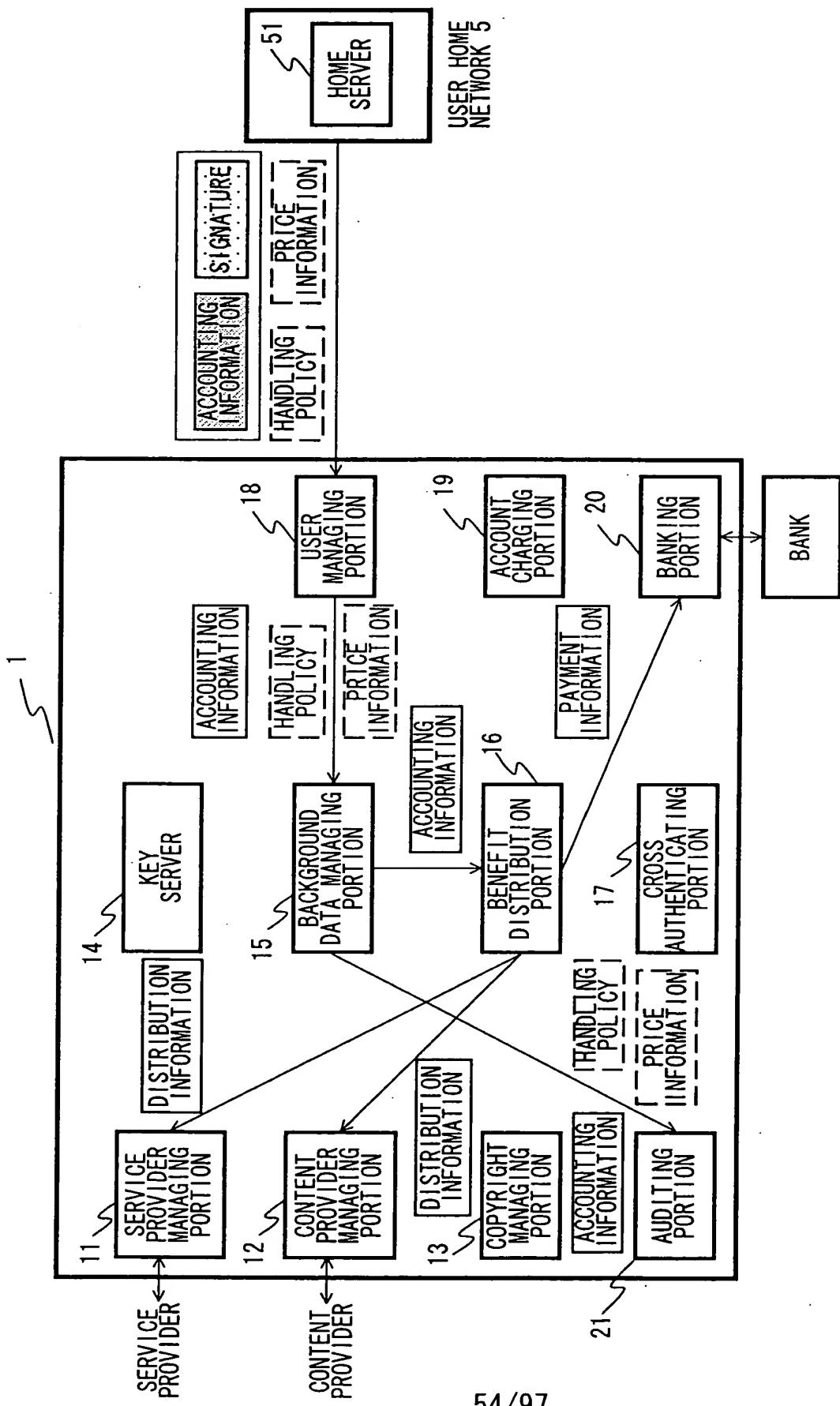


FIG. 53



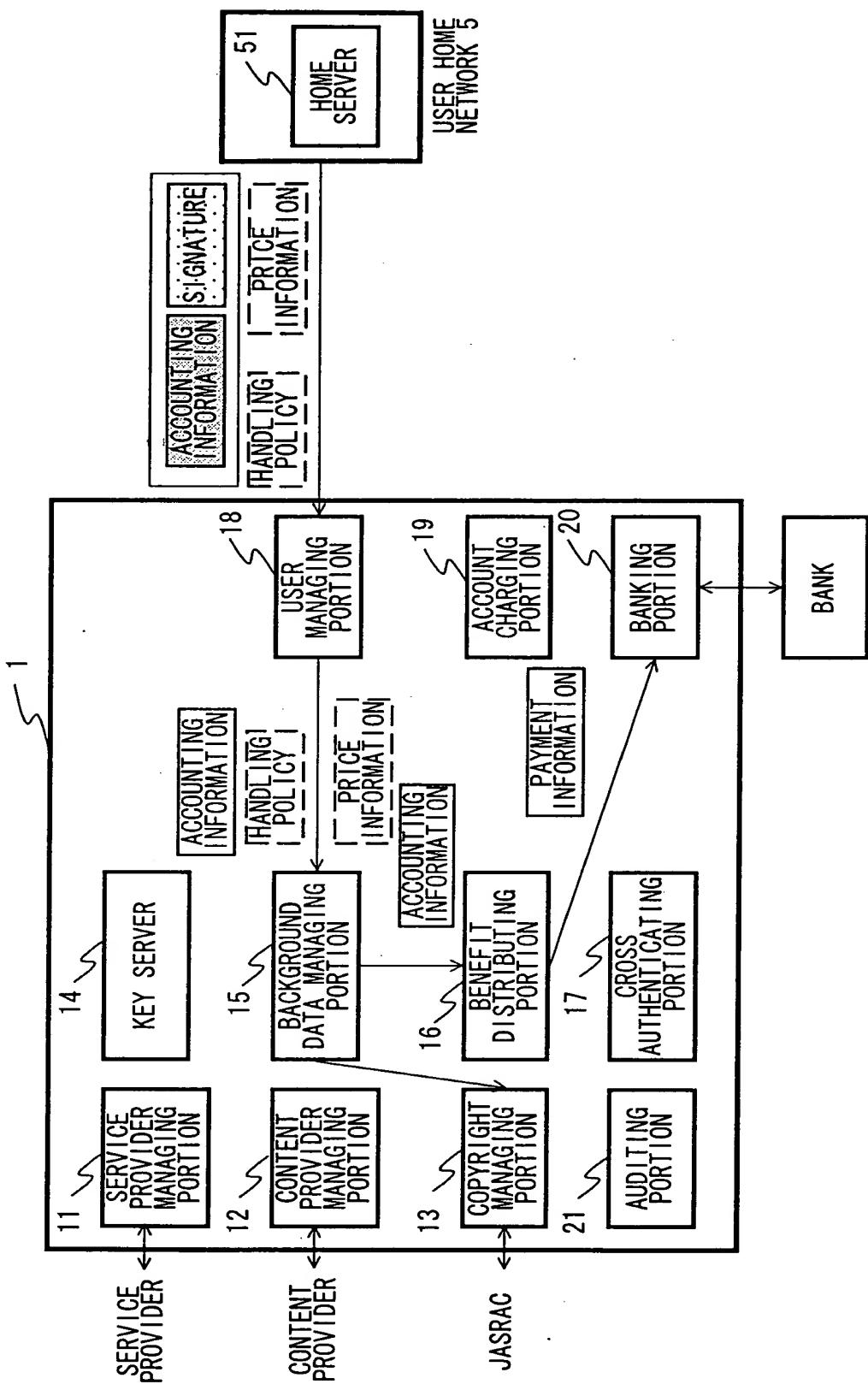


FIG. 55

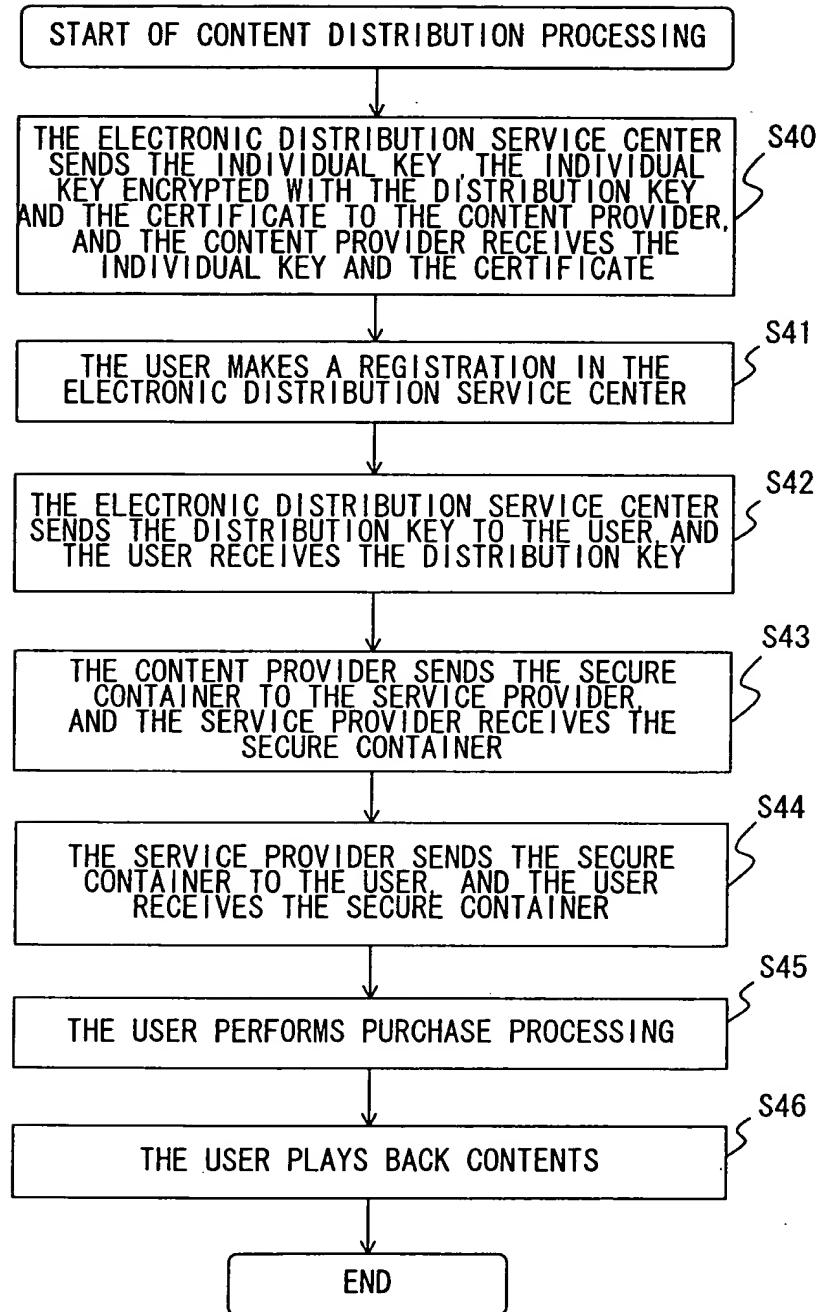


FIG. 56

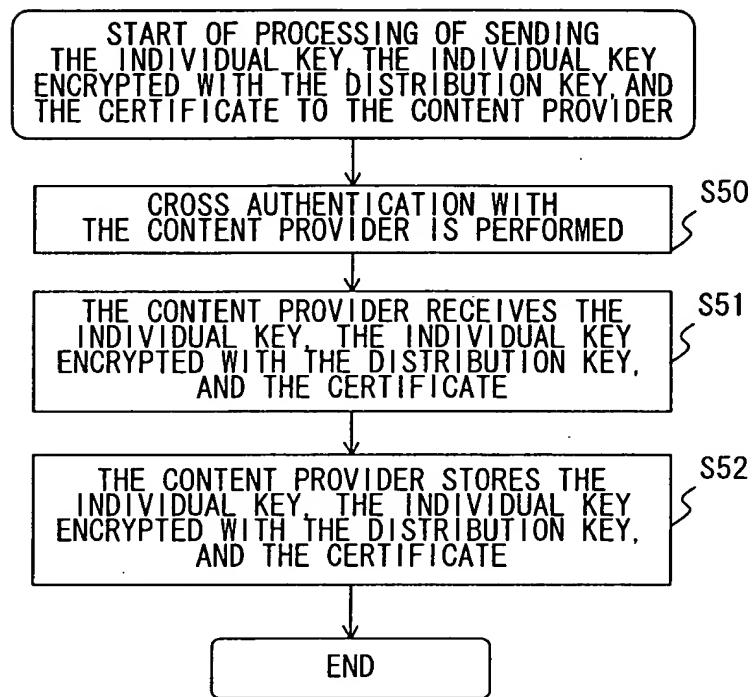


FIG. 57

TOP SECRET EYES ONLY

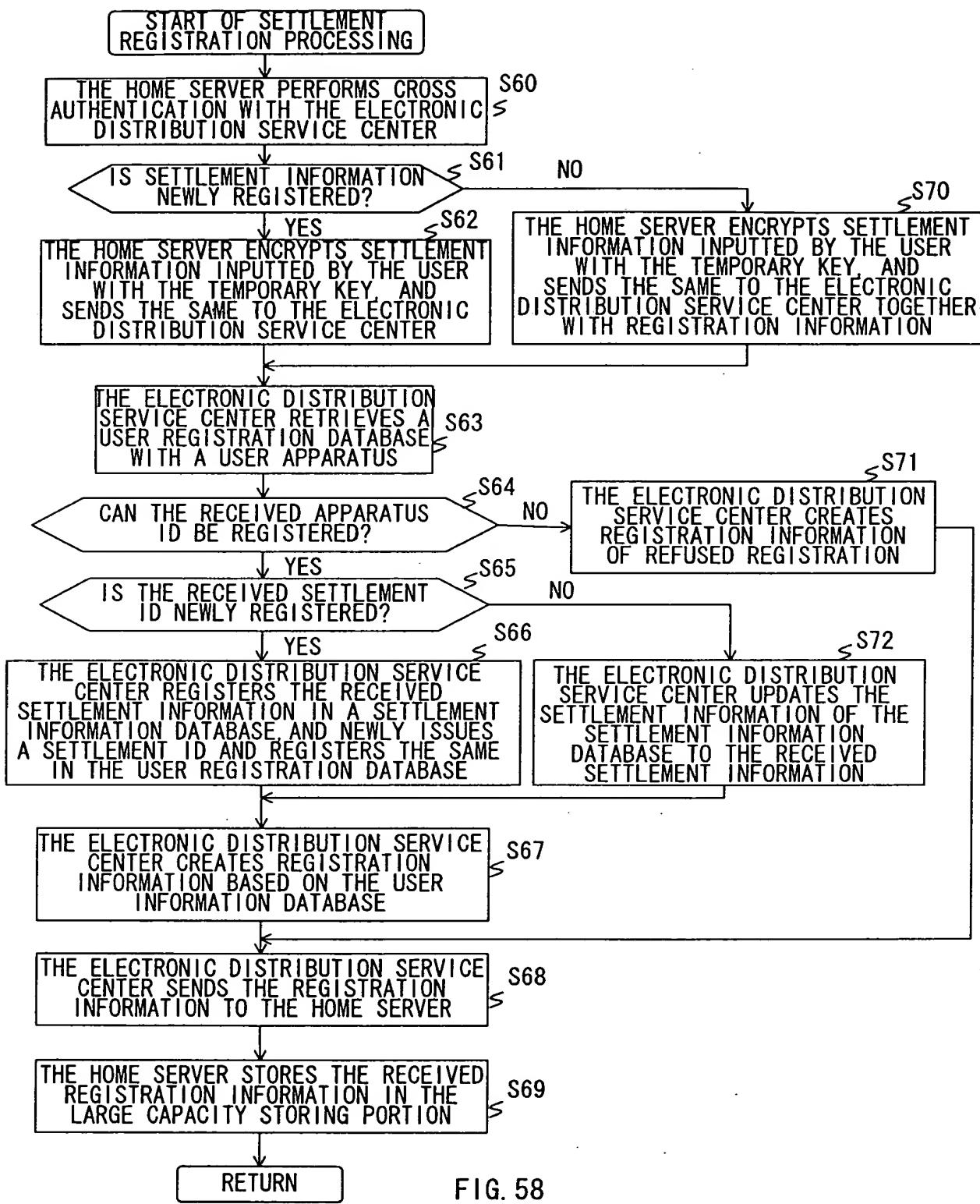


FIG. 58

TOP SECRET//COMINT

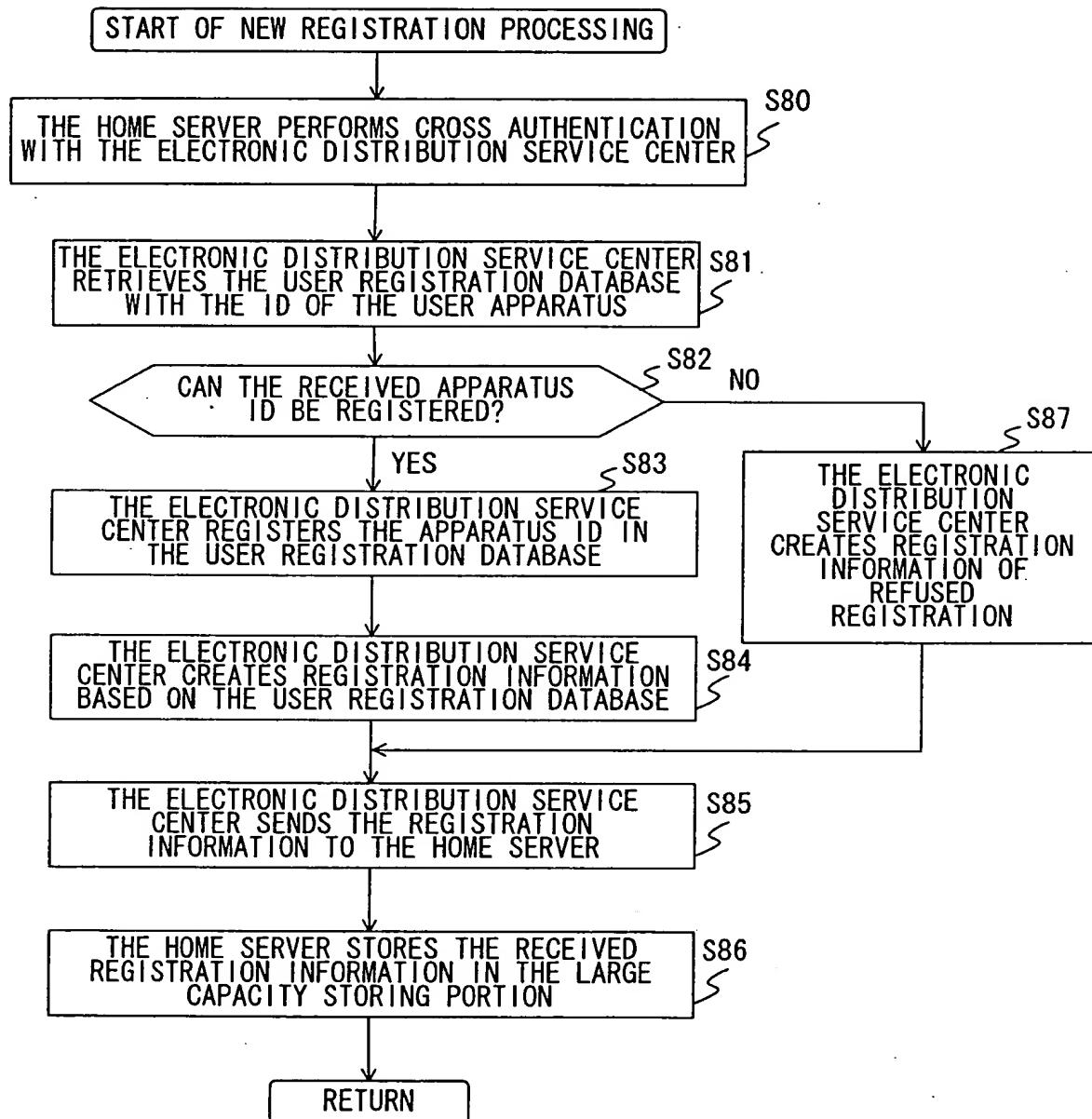


FIG. 59

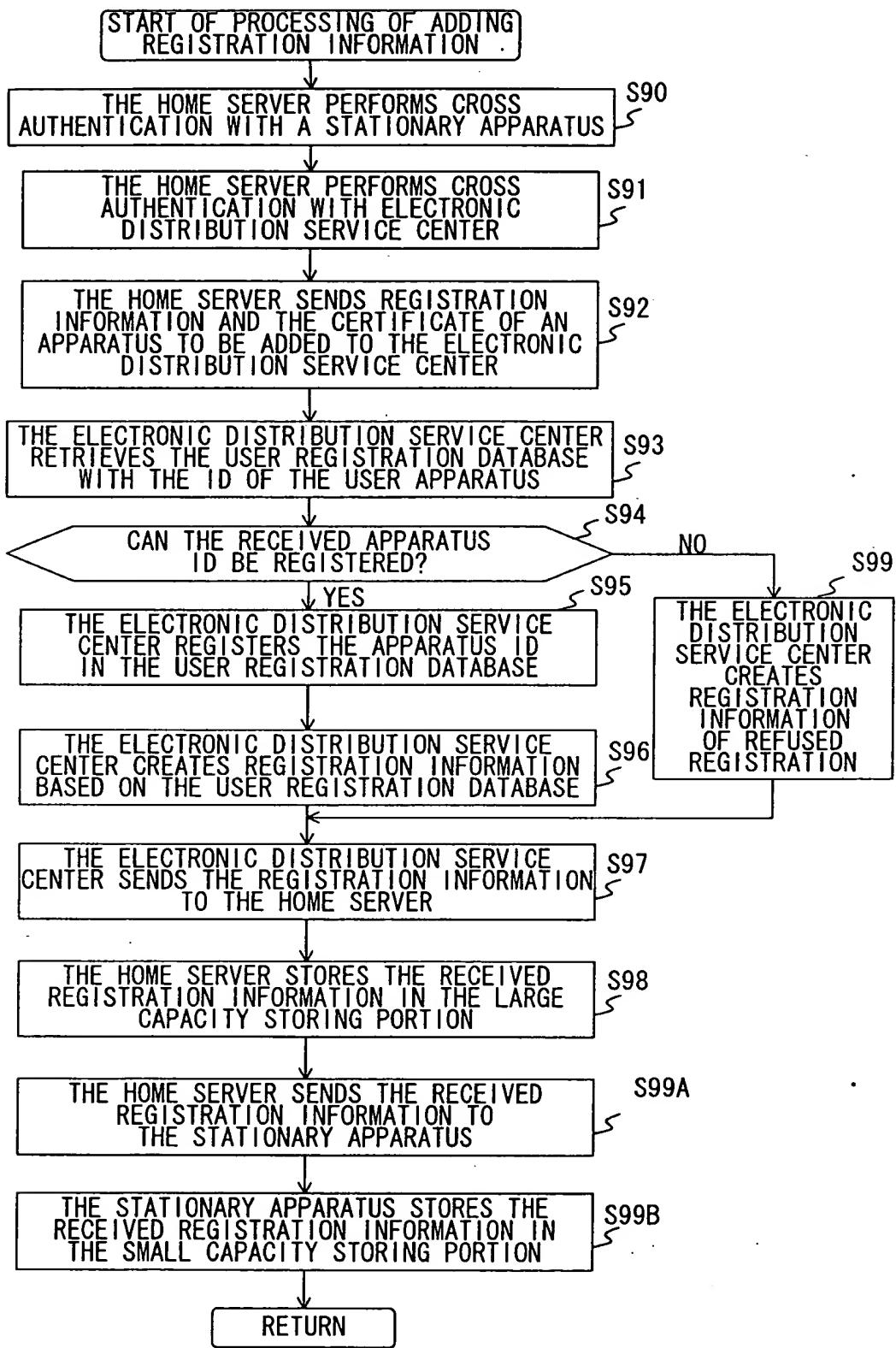


FIG. 60

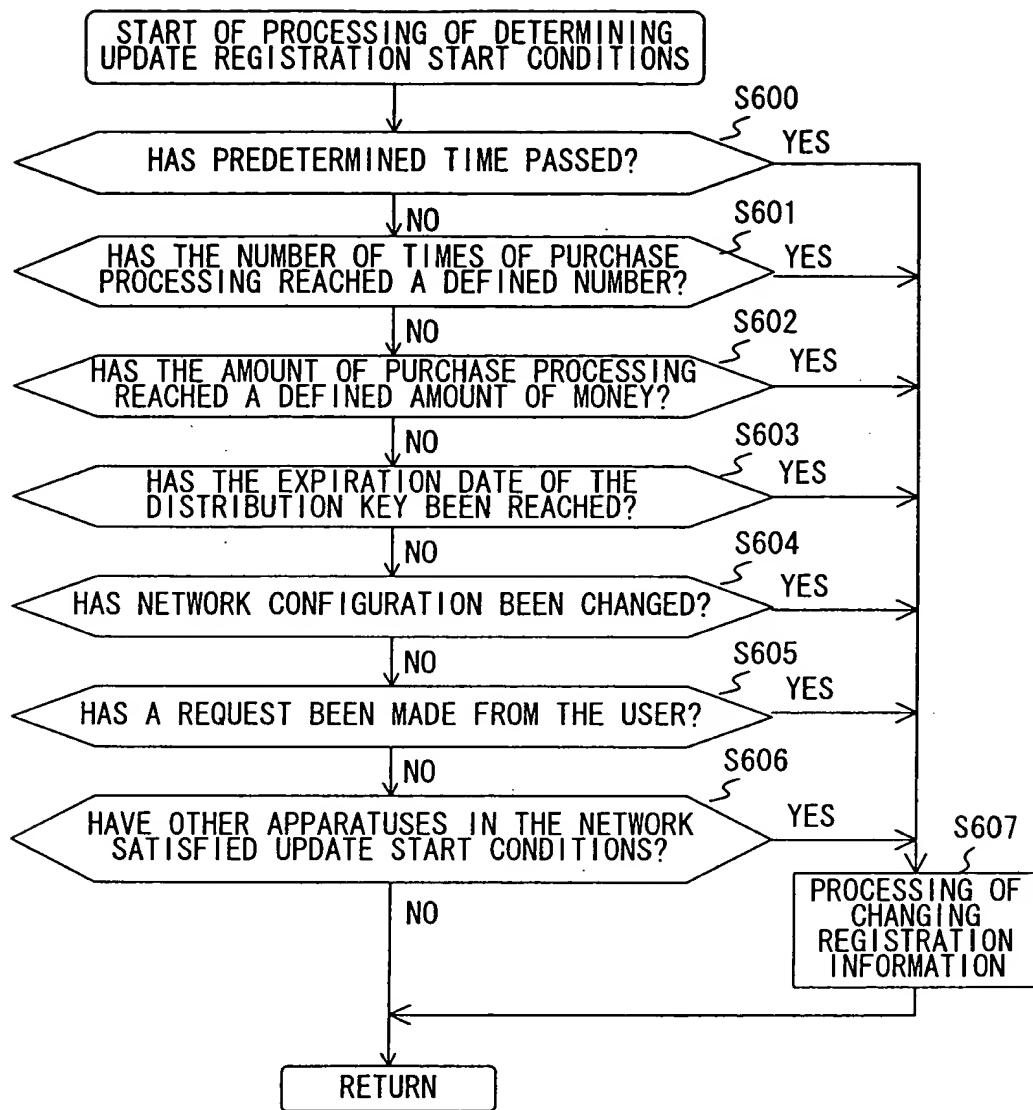


FIG. 61

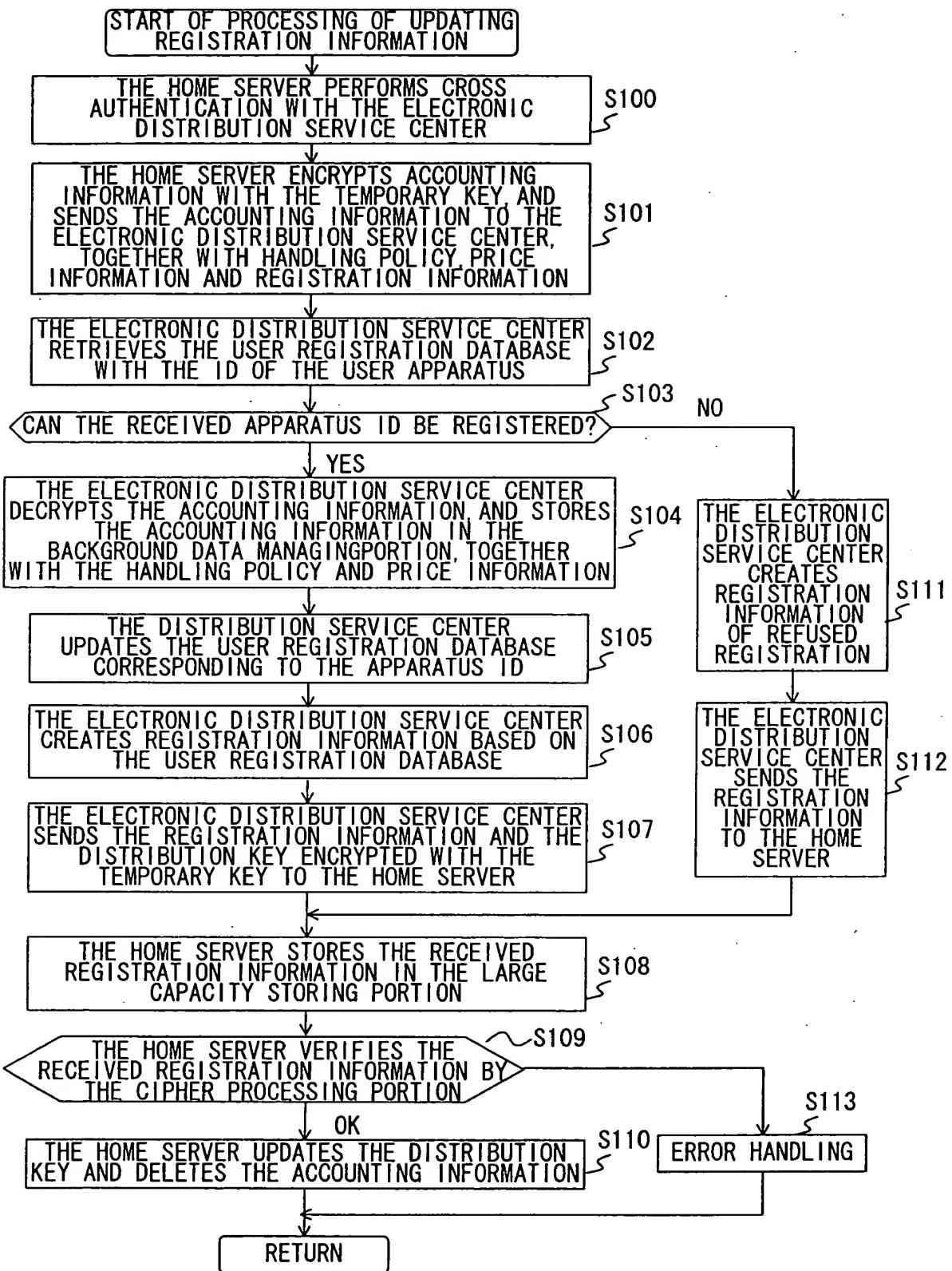


FIG. 62

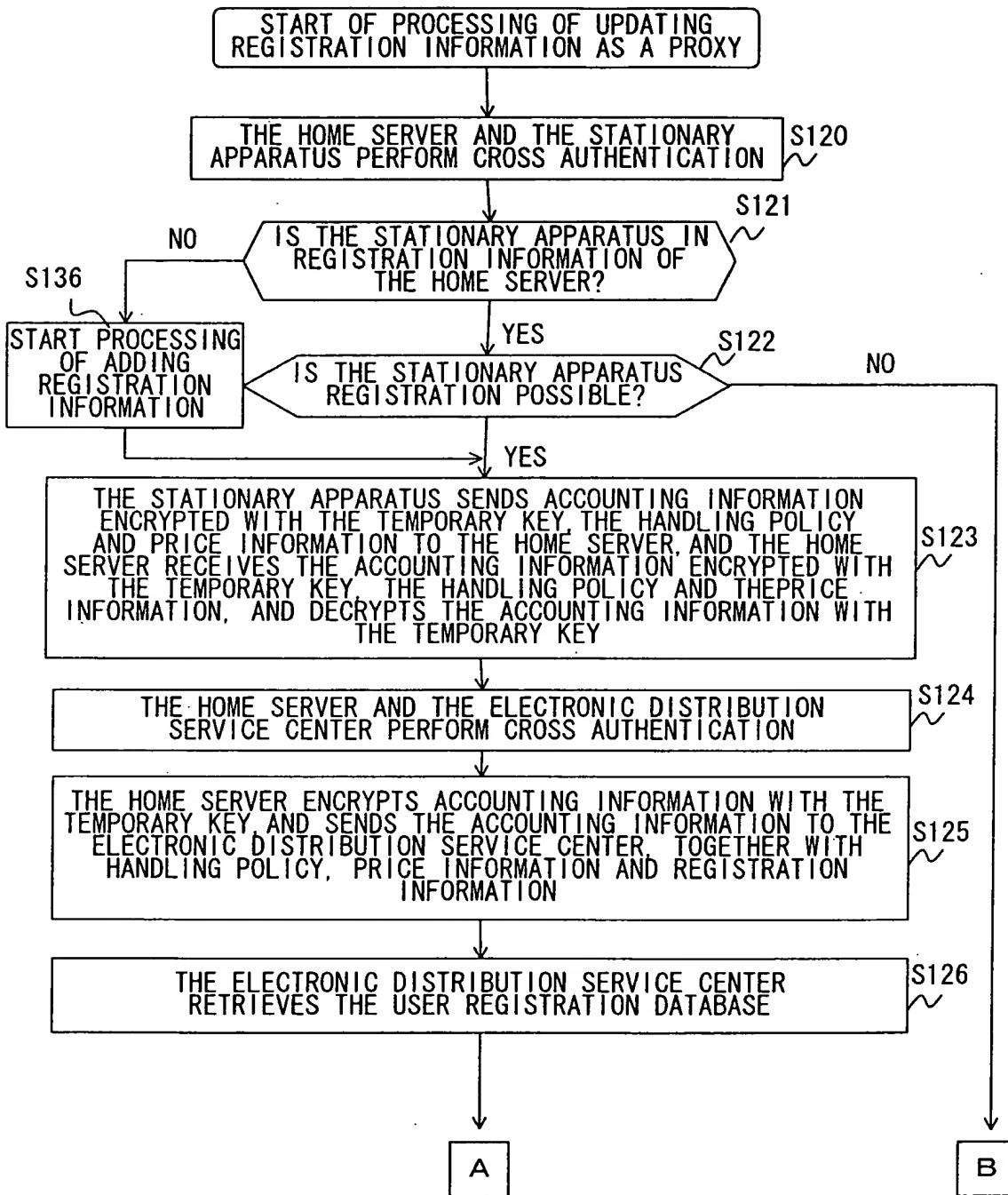


FIG. 63

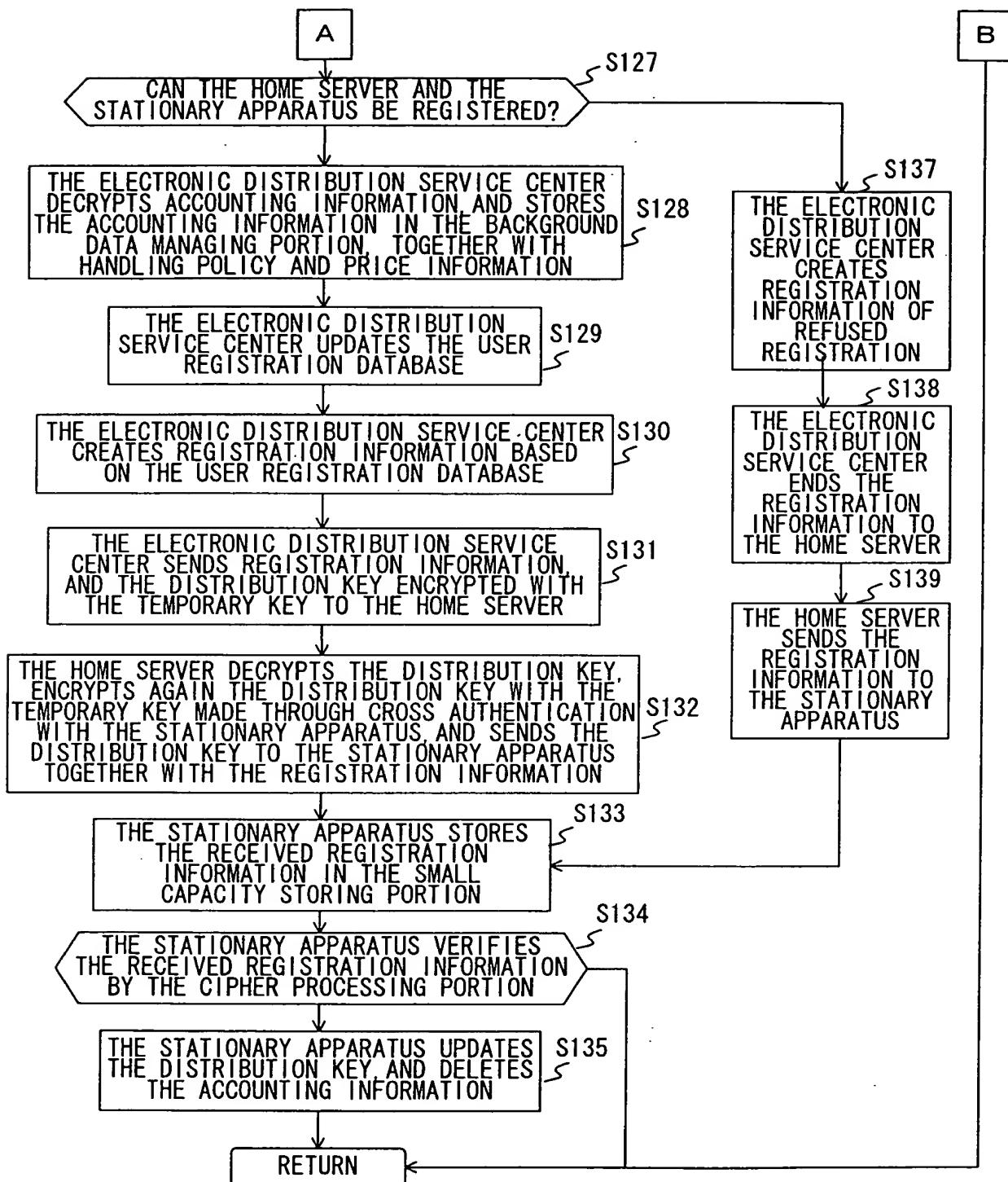


FIG. 64

09930392-201401

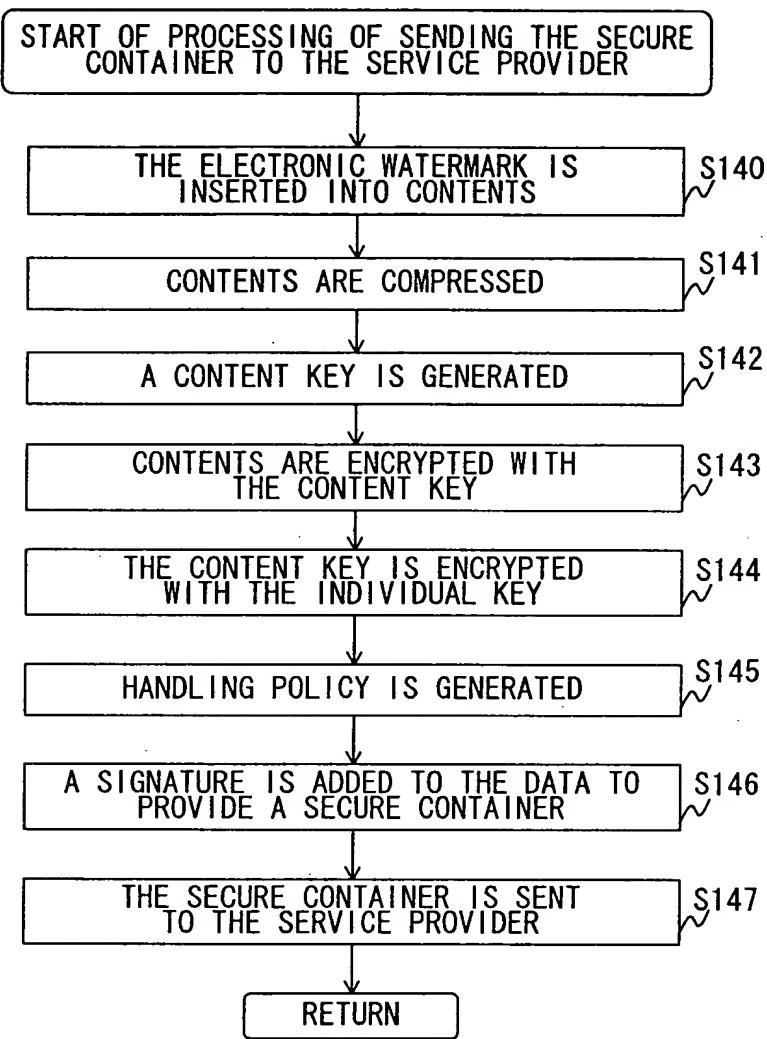


FIG. 65

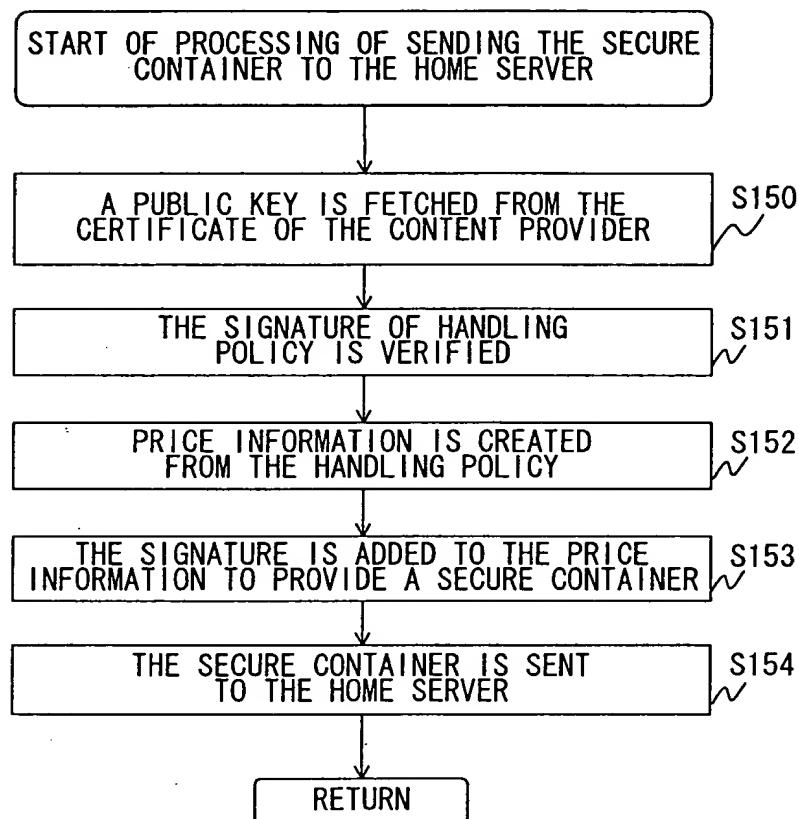


FIG. 66

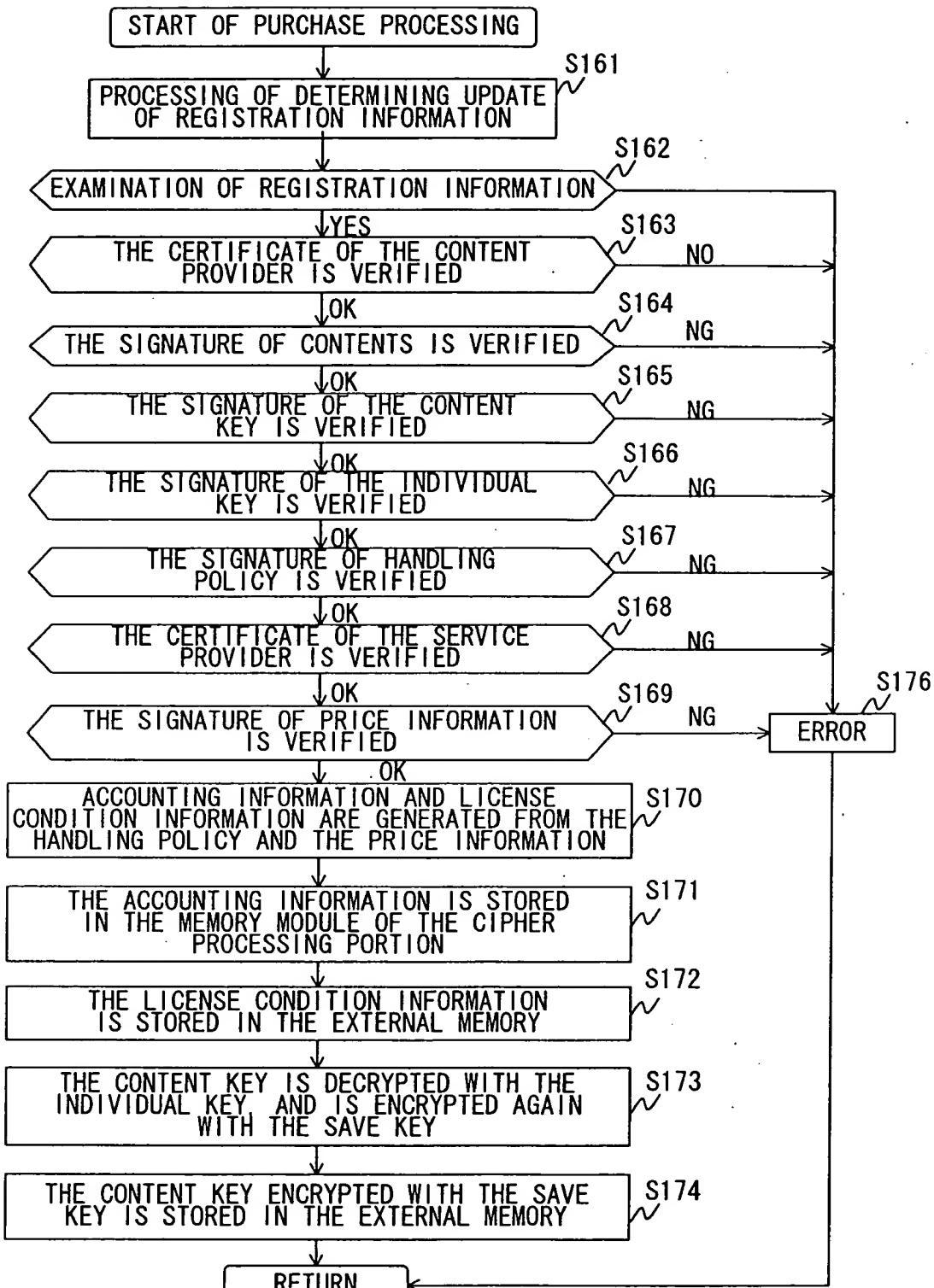


FIG. 67

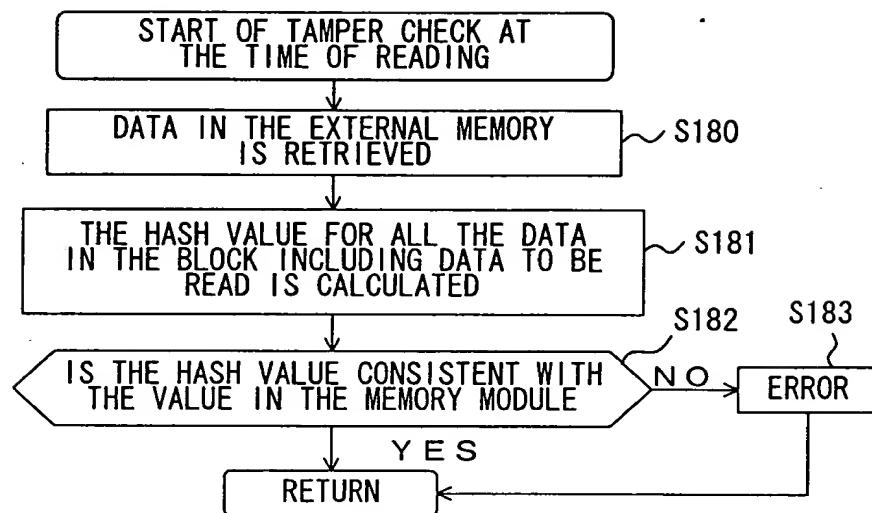


FIG. 68

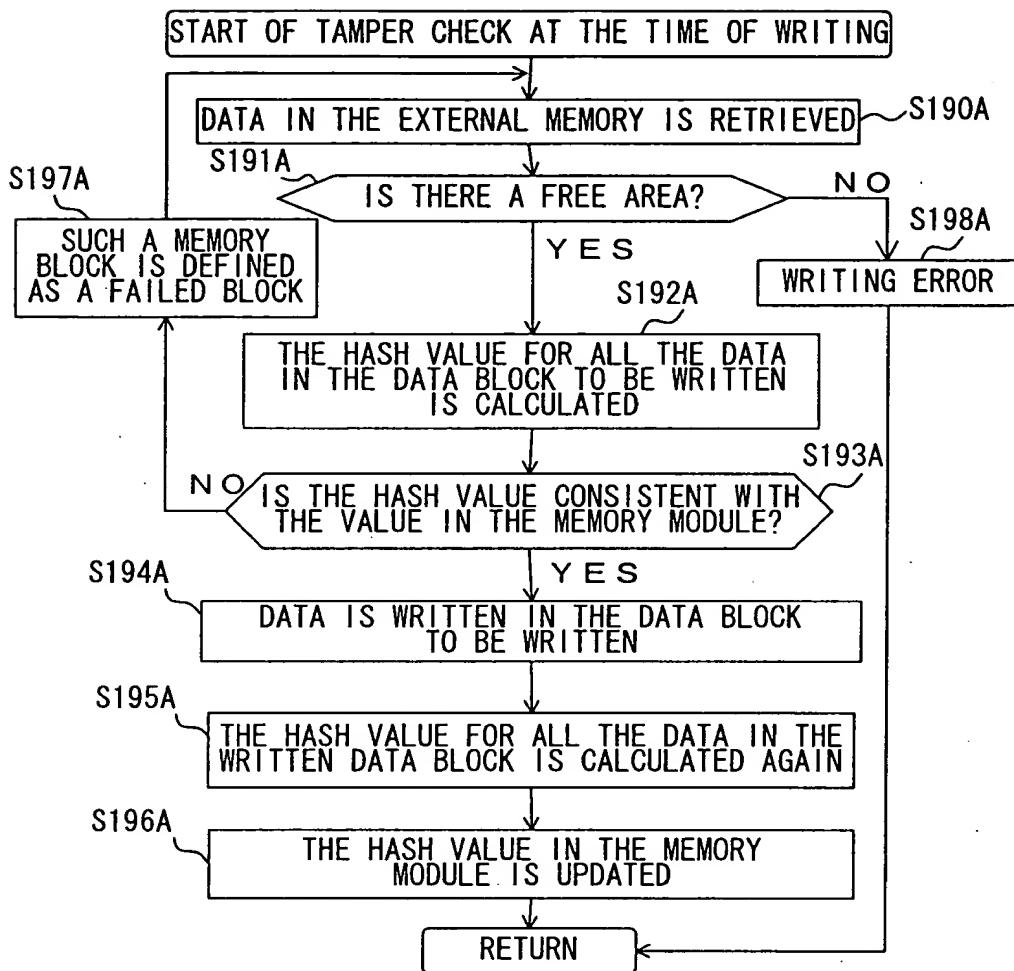


FIG. 69

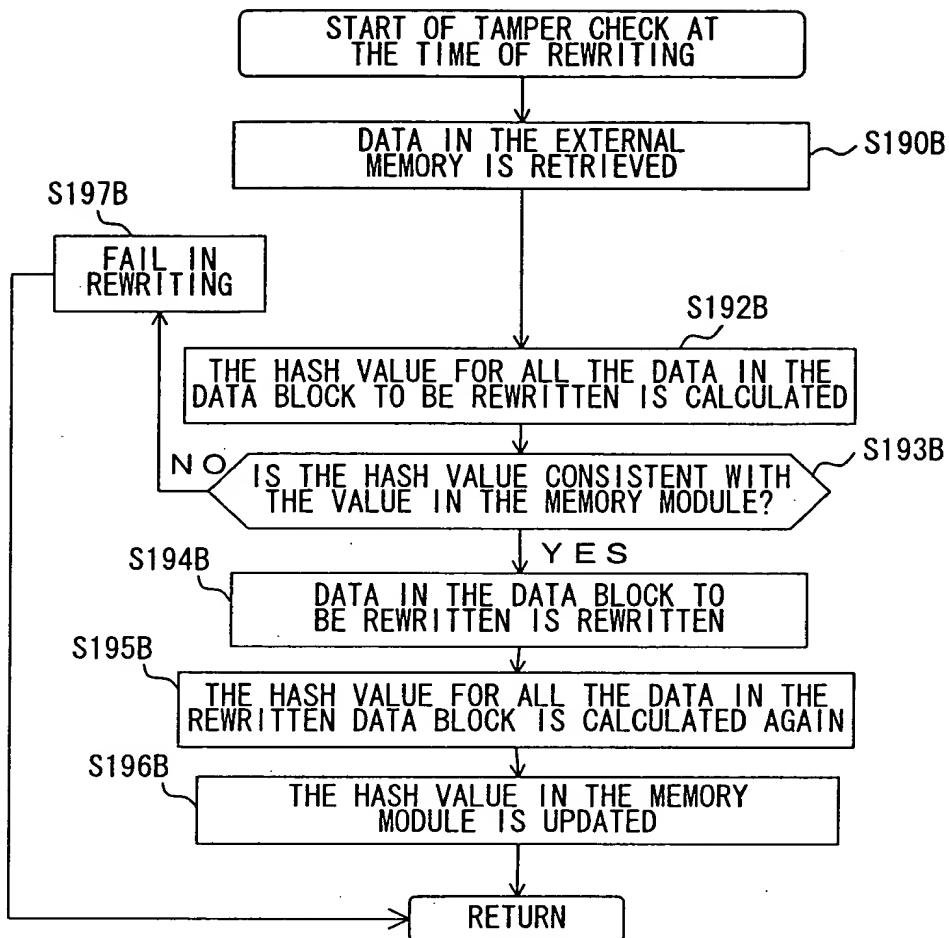


FIG. 70

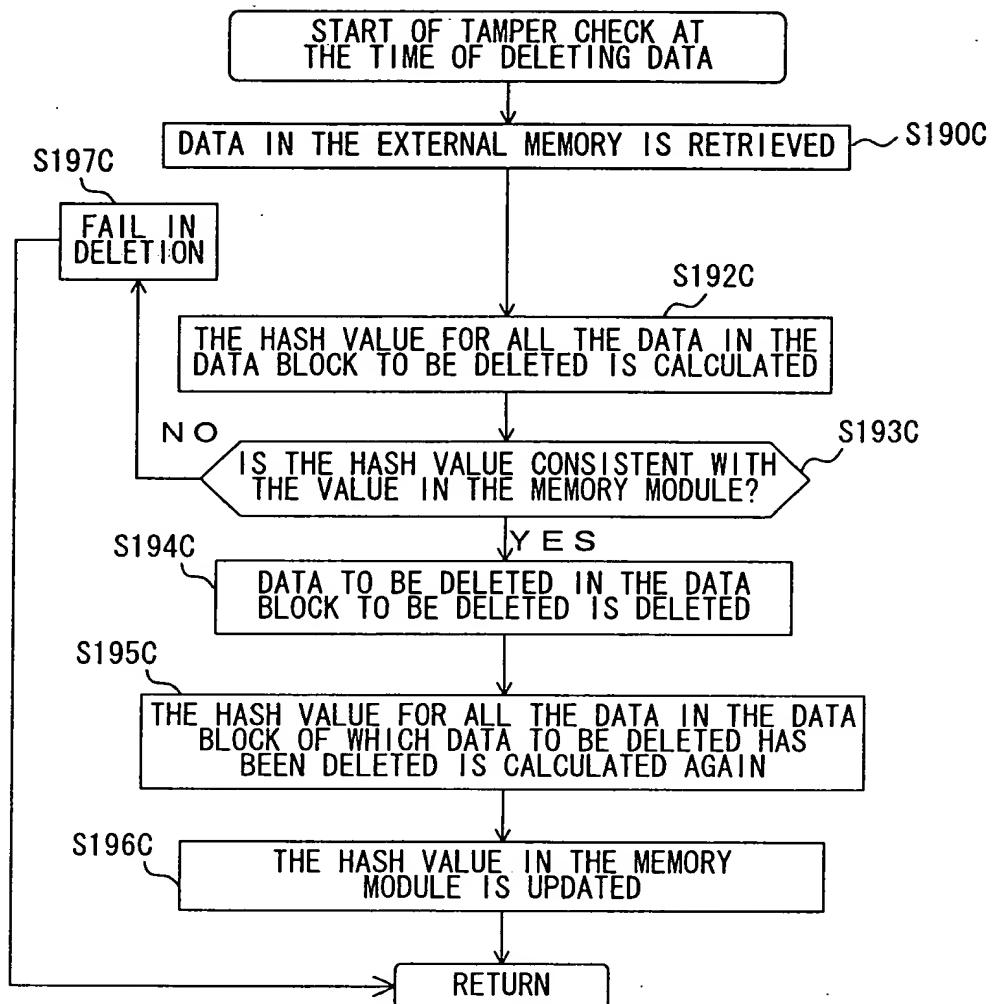


FIG. 71

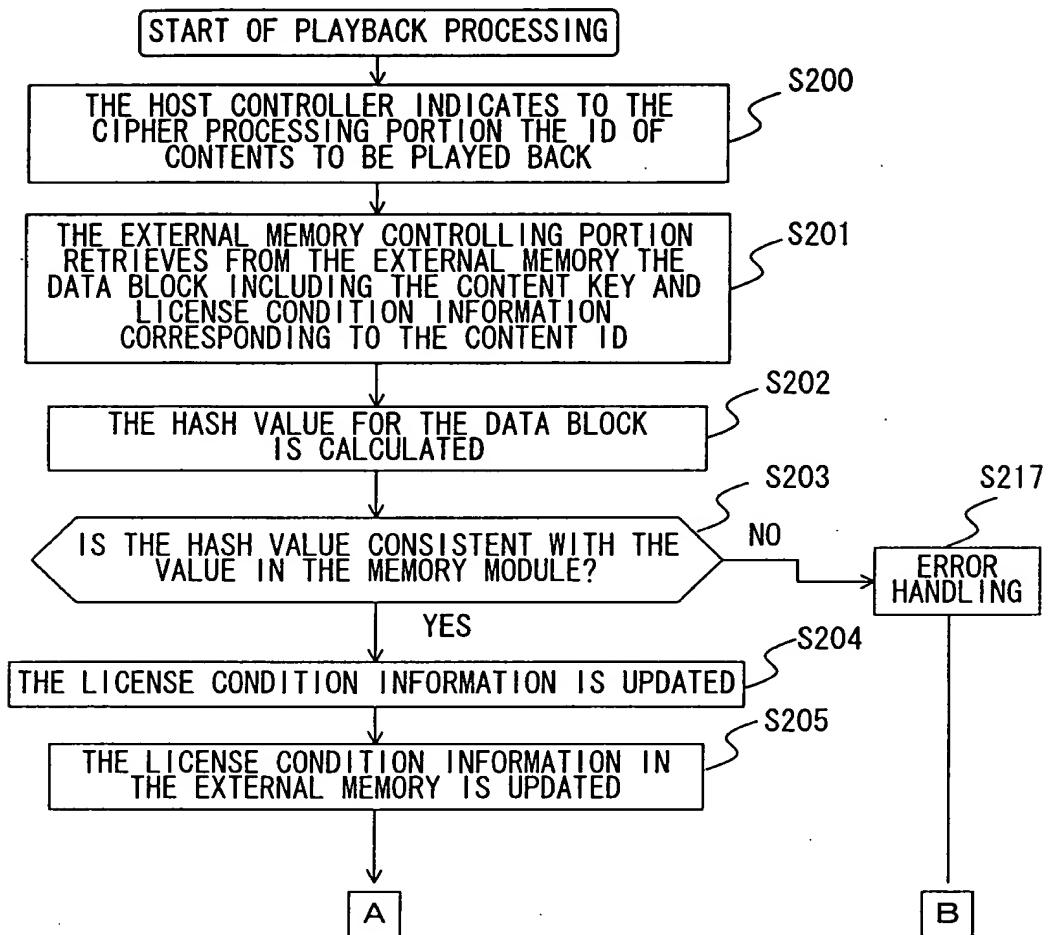


FIG. 72

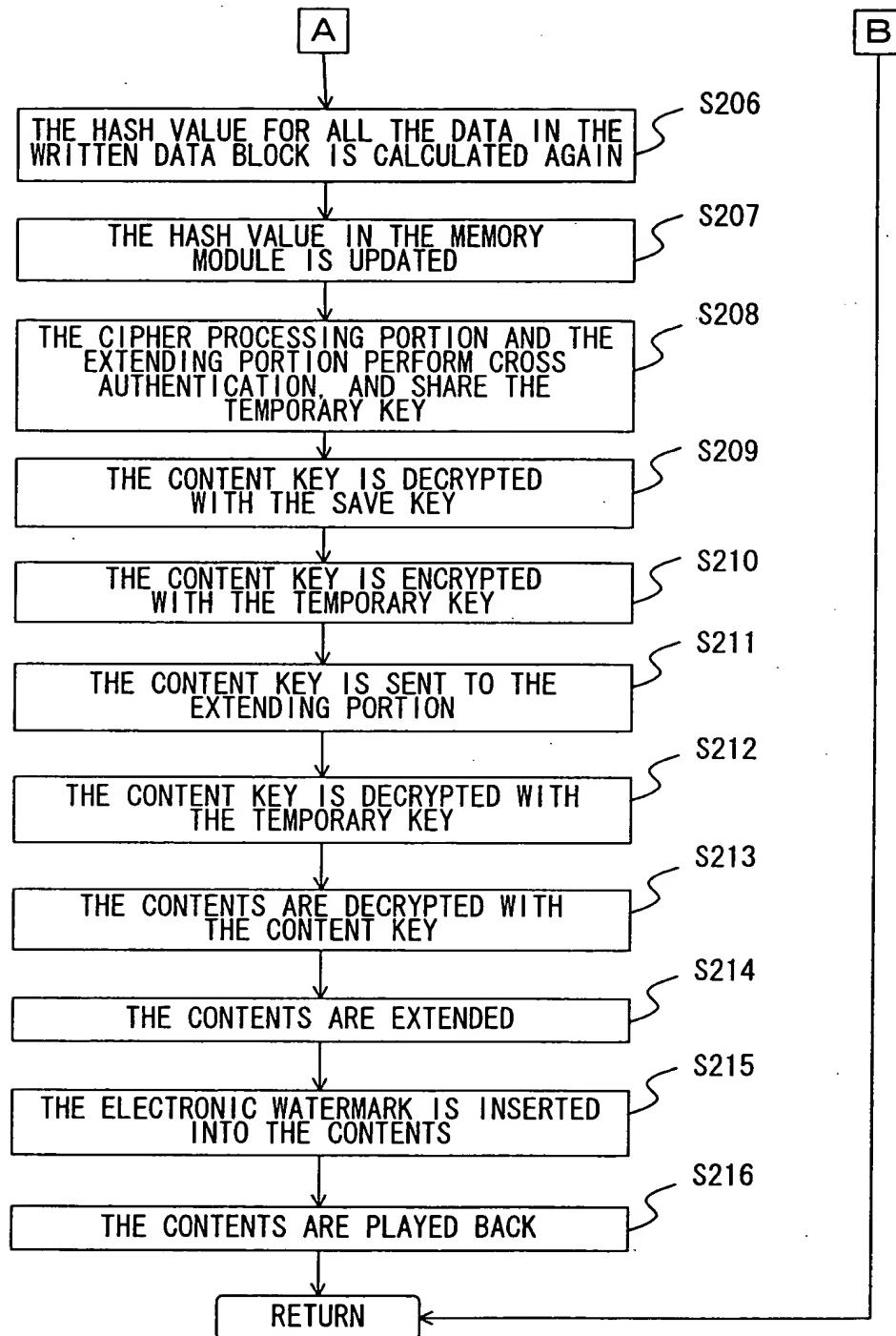


FIG. 73

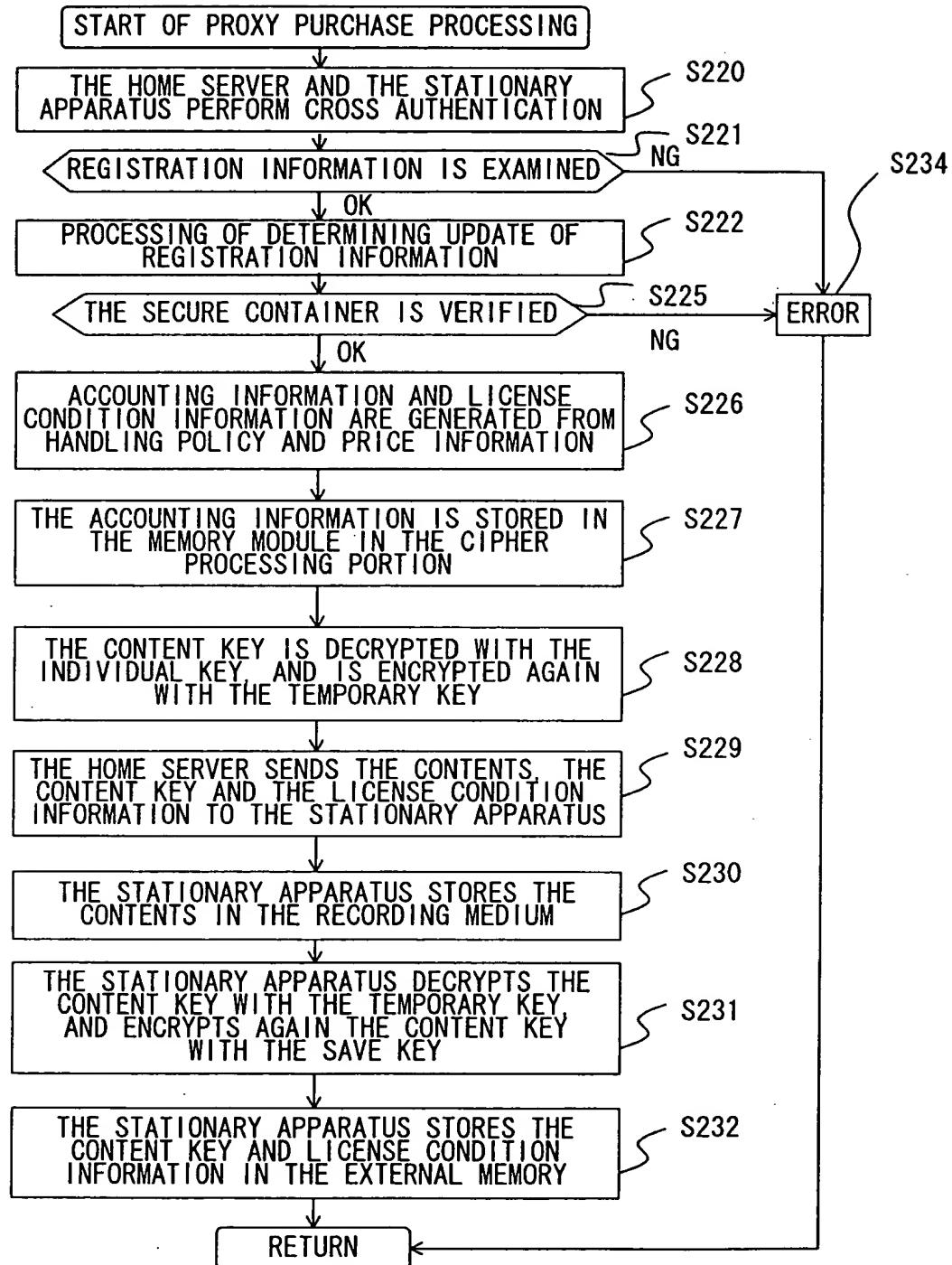


FIG. 74

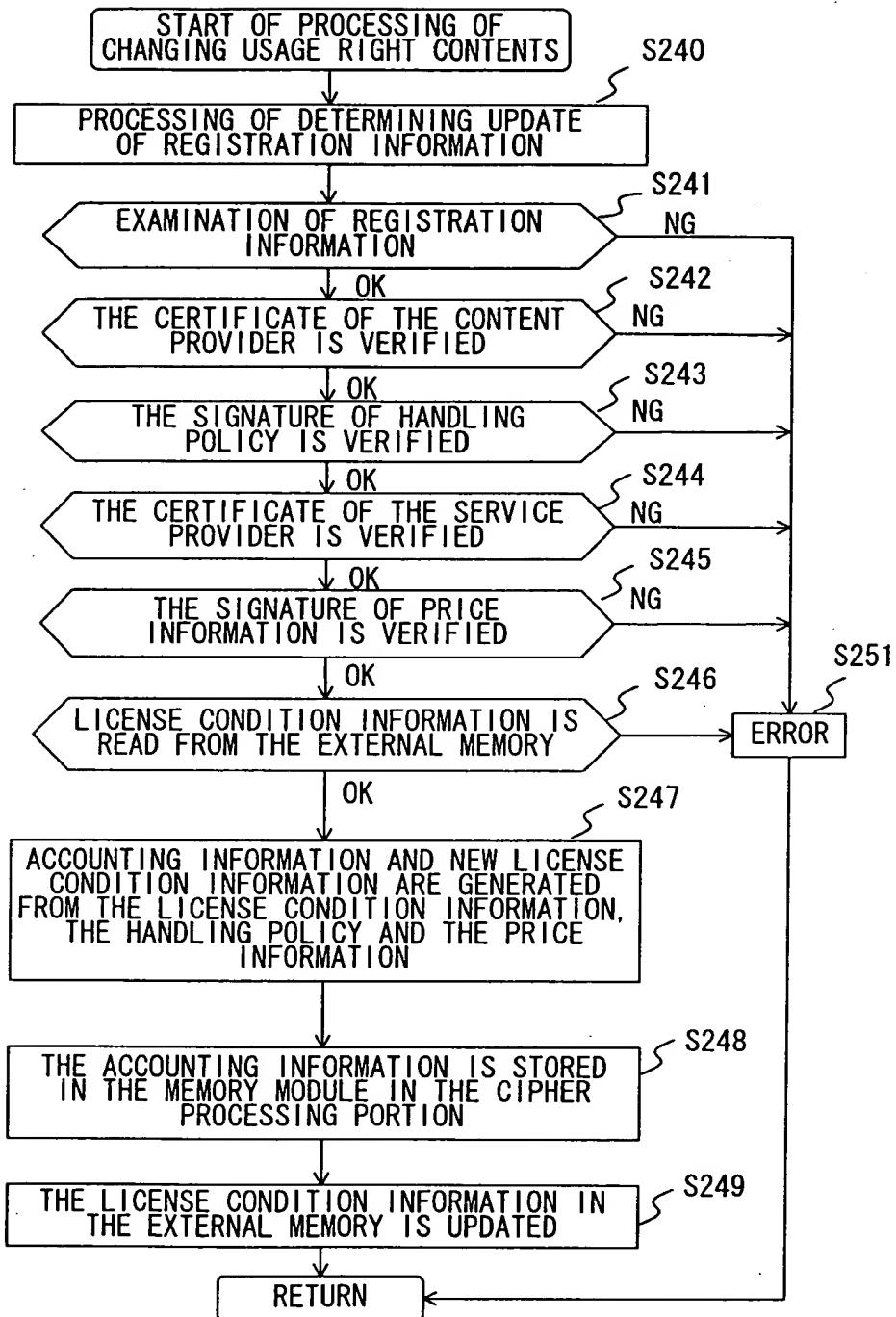


FIG. 75

RULE N	RULE NUMBER
	USAGE CONTENT RIGHT NUMBER
	PARAMETER
	MINIMUM PRICE
	EARNINGS (RATE OF BENEFITS)
RULE 1	RULE NUMBER #1
	USAGE RIGHT CONTENT NUMBER #1
	ABSENT
	¥ 3 5 0
	3 0 %
RULE 2	RULE NUMBER #2
	USAGE RIGHT CONTENT NUMBER #2
	ONE HOUR
	¥ 1 0 0
	3 0 %
RULE 3	RULE NUMBER #3
	USAGE RIGHT CONTENT NUMBER #6
	ONE TIME
	¥ 3 0
	3 0 %
RULE 4	RULE NUMBER #4
	USAGE RIGHT CONTENT NUMBER #13
	# 2 / # 1
	¥ 2 0 0
	2 0 %
RULE 5	RULE NUMBER #5
	USAGE RIGHT CONTENT NUMBER #14
	# 1 / # 1
	¥ 2 5 0
	2 0 %

FIG. 76

09/830392

RULE NUMBER	
PARAMETER	
PRICE	
RULE N	RULE #1
1	RULE NUMBER #1
	30%
	¥ 500
RULE N	RULE #2
2	RULE NUMBER #2
	40%
	¥ 100
RULE N	RULE #3
3	RULE NUMBER #3
	40%
	¥ 100
RULE N	RULE #4
4	RULE NUMBER #4
	10%
	¥ 200
RULE N	RULE #5
5	RULE NUMBER #5
	20%
	¥ 350

FIG. 77

RULE 1	# 1
	# 1
	ABSENT
RULE 2	¥ 350
	30%
	# 2
RULE 3	# 2
	ONE HOUR
	¥ 100
	30%
	# 3
	# 13
	# 2 / # 1
	¥ 200
	20%

ONE PART OF RULE PART  
OF HANDLING POLICY

PRESENT

RULE	RULE NUMBER
	USAGE RIGHT CONTENT NUMBER
	PARAMETER
RULE	# 2
	# 2
	THIRTY MINUTES / TWO HOURS

RULE PART OF LICENSE  
CONDITION INFORMATION

RULE 1	# 1
	30%
	¥ 500
RULE 2	# 2
	40%
	¥ 100
RULE 3	# 3
	10%
	¥ 200

ONE PART OF RULE PART  
OF PRICE INFORMATION

AFTER CHANGE

RULE	RULE NUMBER
	USAGE RIGHT CONTENT NUMBER
	PARAMETER
RULE	# 1
	# 1
	ABSENT

RULE PART OF LICENSE  
CONDITION INFORMATION

FIG. 78

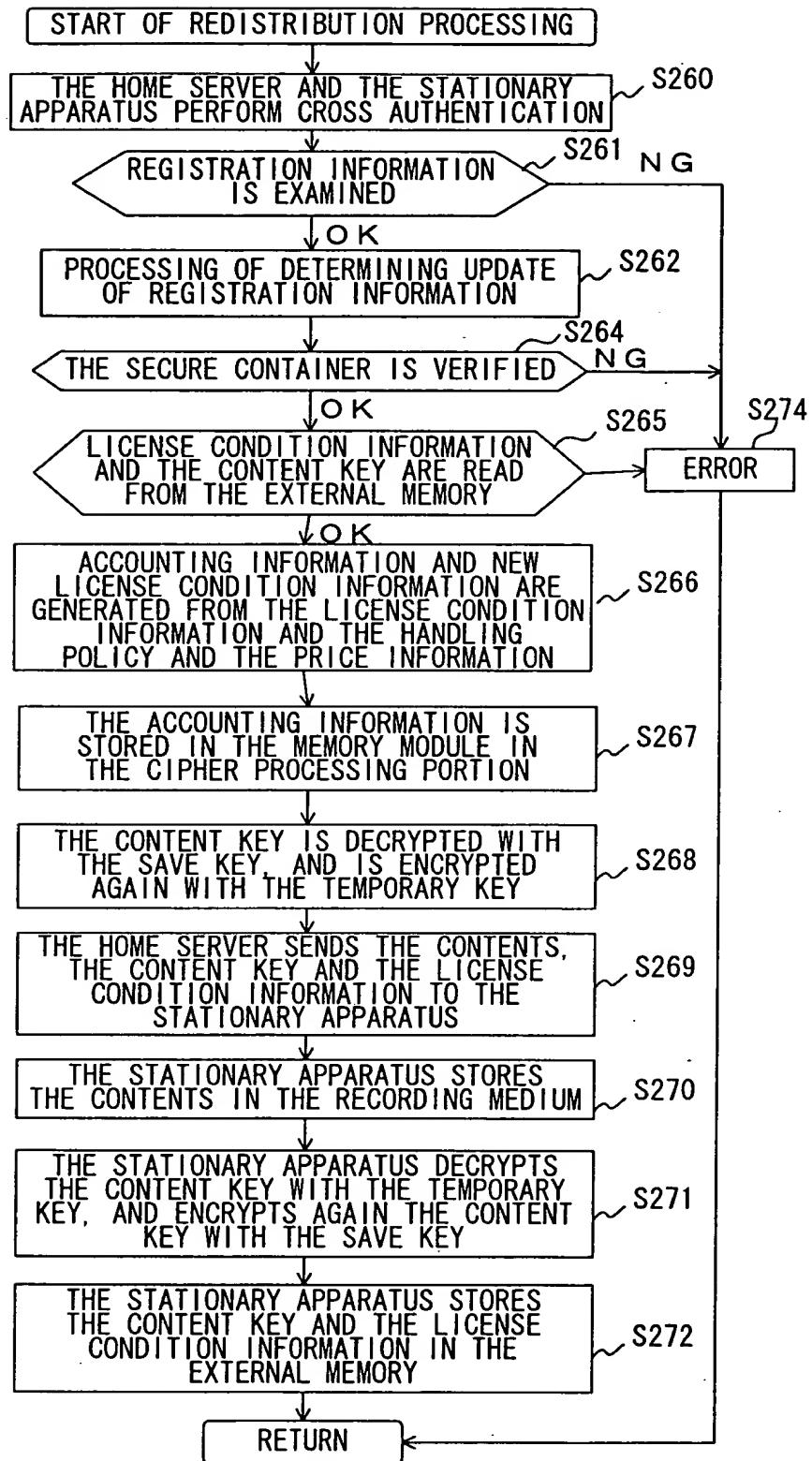


FIG. 79

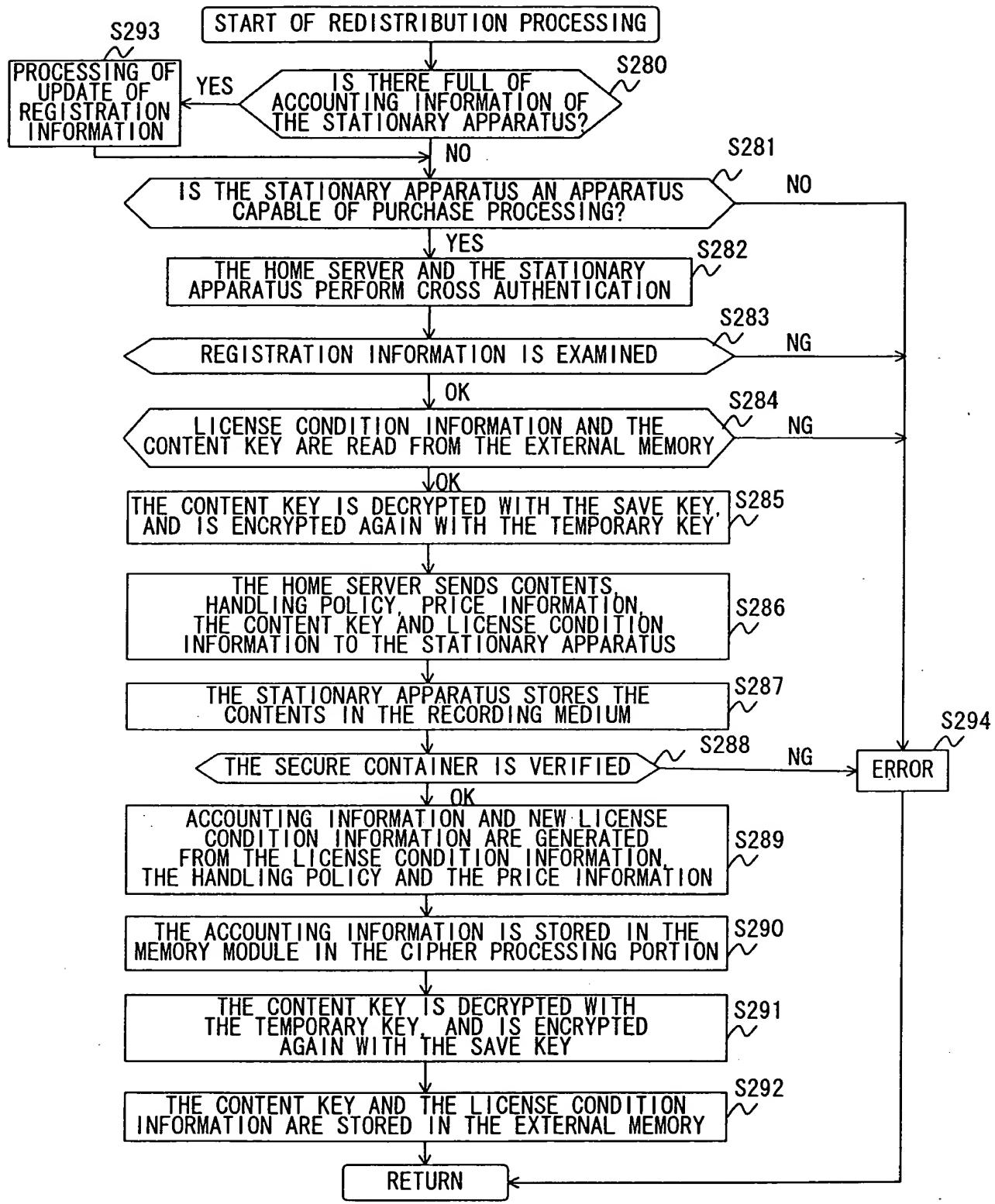


FIG. 80

RULE 1	RULE NUMBER #1	
	USAGE RIGHT CONTENT NUMBER #1	
	ABSENT	
	¥ 350	
	30%	
RULE 2	RULE NUMBER #2	
	USAGE RIGHT CONTENT NUMBER #16	
	ABSENT	
	¥ 100	
	50%	

ONE PART OF RULE PART  
OF HANDLING POLICY

RULE 1	RULE NUMBER #1	
	30%	
RULE 2	¥ 500	
	RULE NUMBER #2	
RULE 2	0%	
	¥ 100	

ONE PART OF RULE PART  
OF PRICE INFORMATION

RULE	RULE NUMBER #1		RULE NUMBER #1 (RULE NUMBER)
	ID 1	ID 1 (ID OF CIPHER PROCESSING PORTION)	
	ABSENT	—	(ID OF CIPHER PROCESSING PORTION HAVING PLAYBACK RIGHT)

INITIAL CONDITION :  
PLAYBACK RIGHT WITH NO LIMIT ON TIME AND THE  
NUMBER OF TIMES, WITH NO MANAGEMENT TRANSFER RIGHT

RULE	RULE NUMBER #1		AFTER PURCHASE OF MANAGEMENT TRANSFER RIGHT : PLAYBACK RIGHT WITH NO LIMIT ON TIME AND THE NUMBER OF TIMES WITH MANAGEMENT TRANSFER RIGHT (PURCHASER / POSSESSOR)
	ID 1		
	PRESENT	ID 1	

RULE	RULE NUMBER #1	
	ID 1	
	PRESENT	ID 2

AFTER TRANSFER OF MANAGEMENT  
TRANSFER RIGHT :  
ONE PART OF LICENSE CONDITION  
INFORMATION OF SENDING END (ID 1)

RULE	RULE NUMBER #1	
	ID 1	
	PRESENT	ID 2

AFTER TRANSFER OF MANAGEMENT  
TRANSFER RIGHT :  
ONE PART OF LICENSE CONDITION  
INFORMATION OF RECEIVING END (ID 2)

FIG. 81

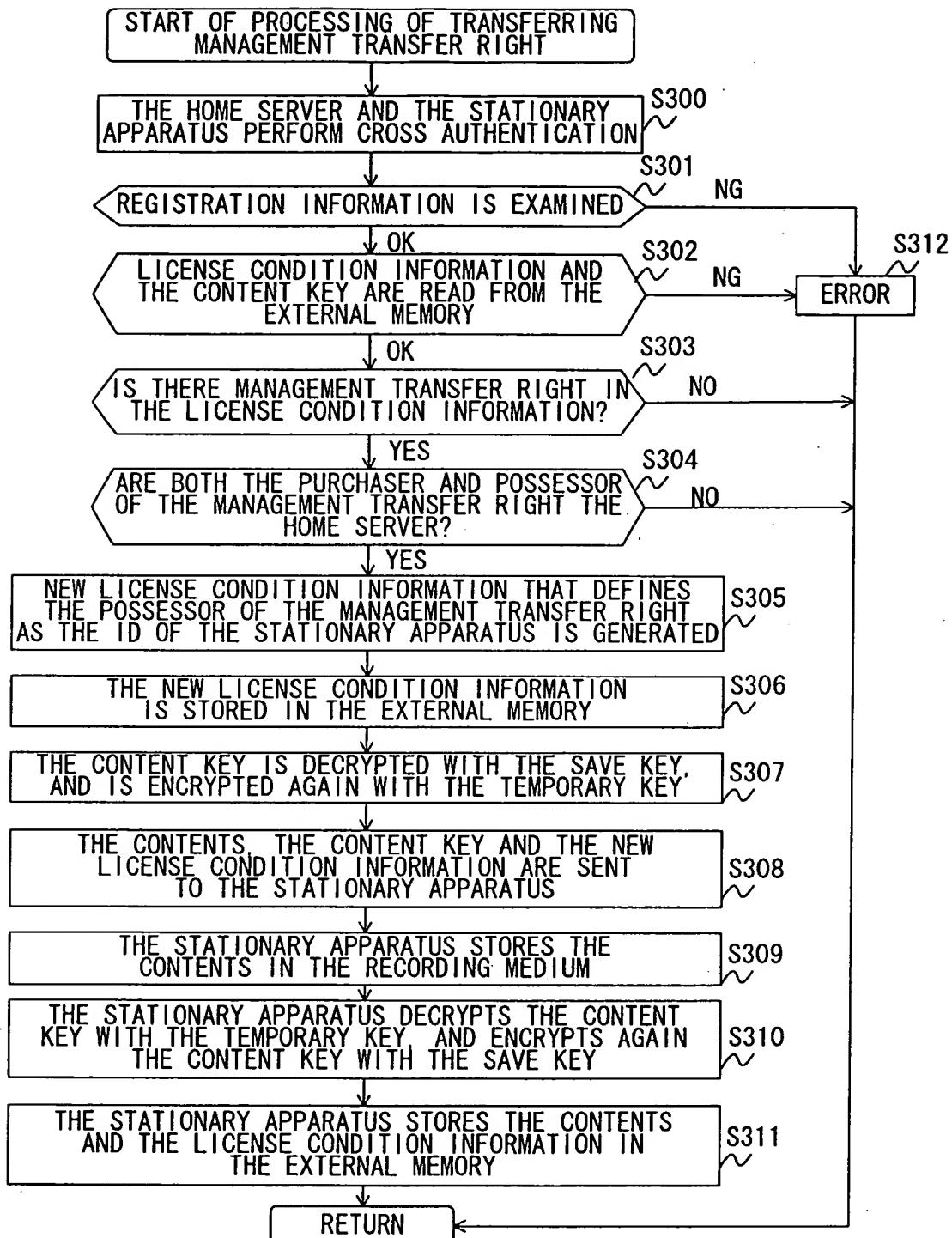


FIG. 82

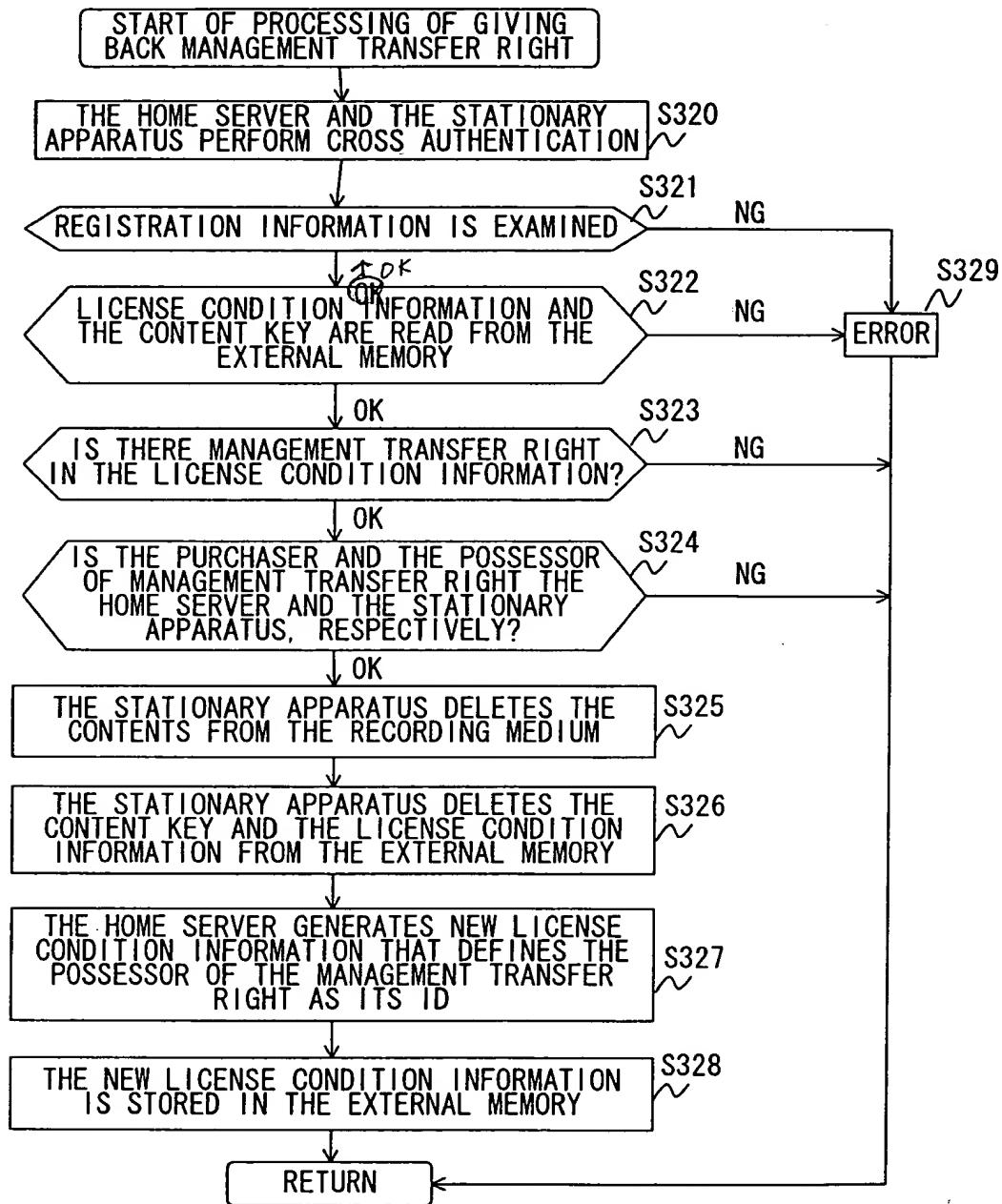


FIG. 83

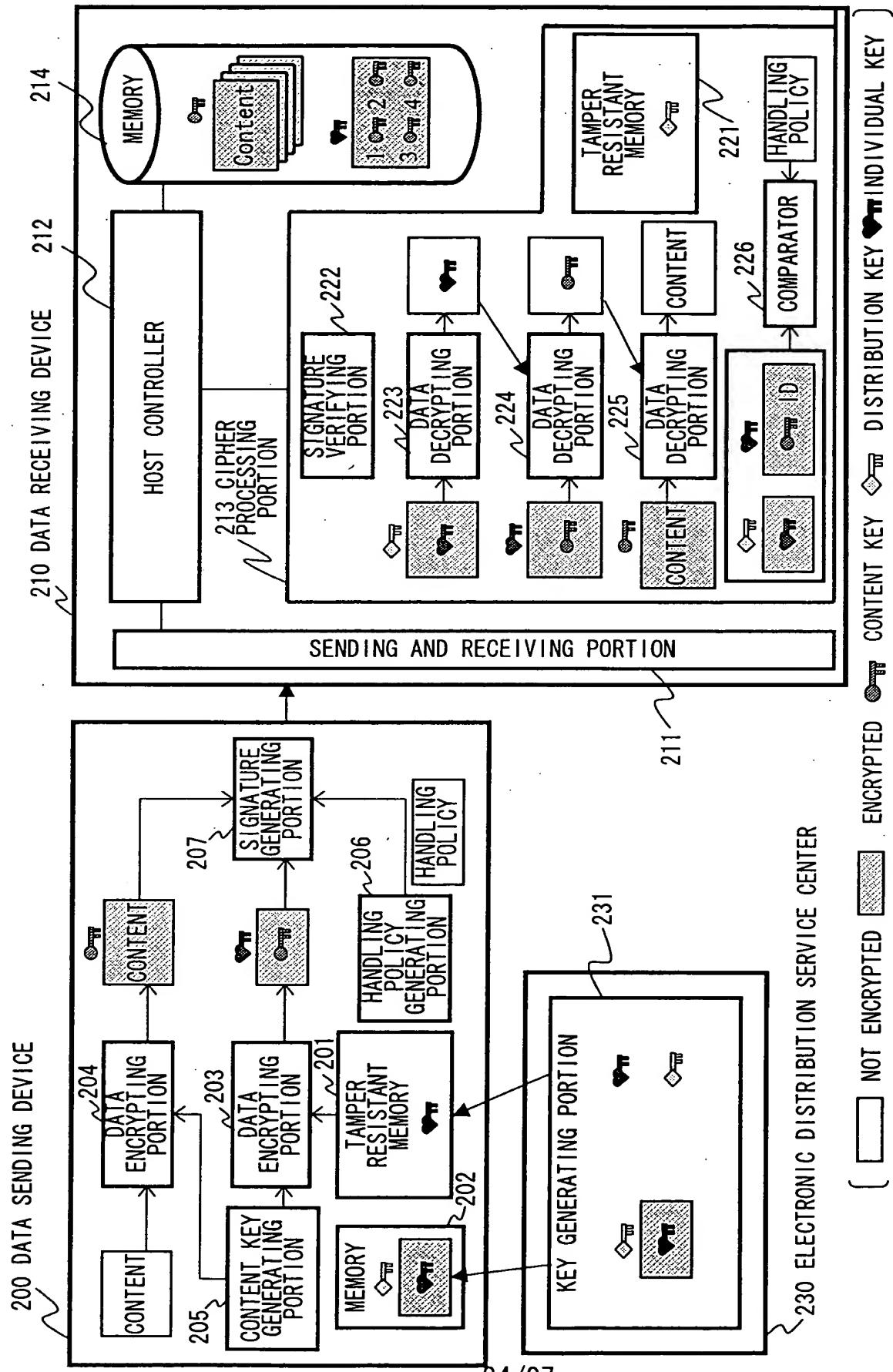


FIG. 84

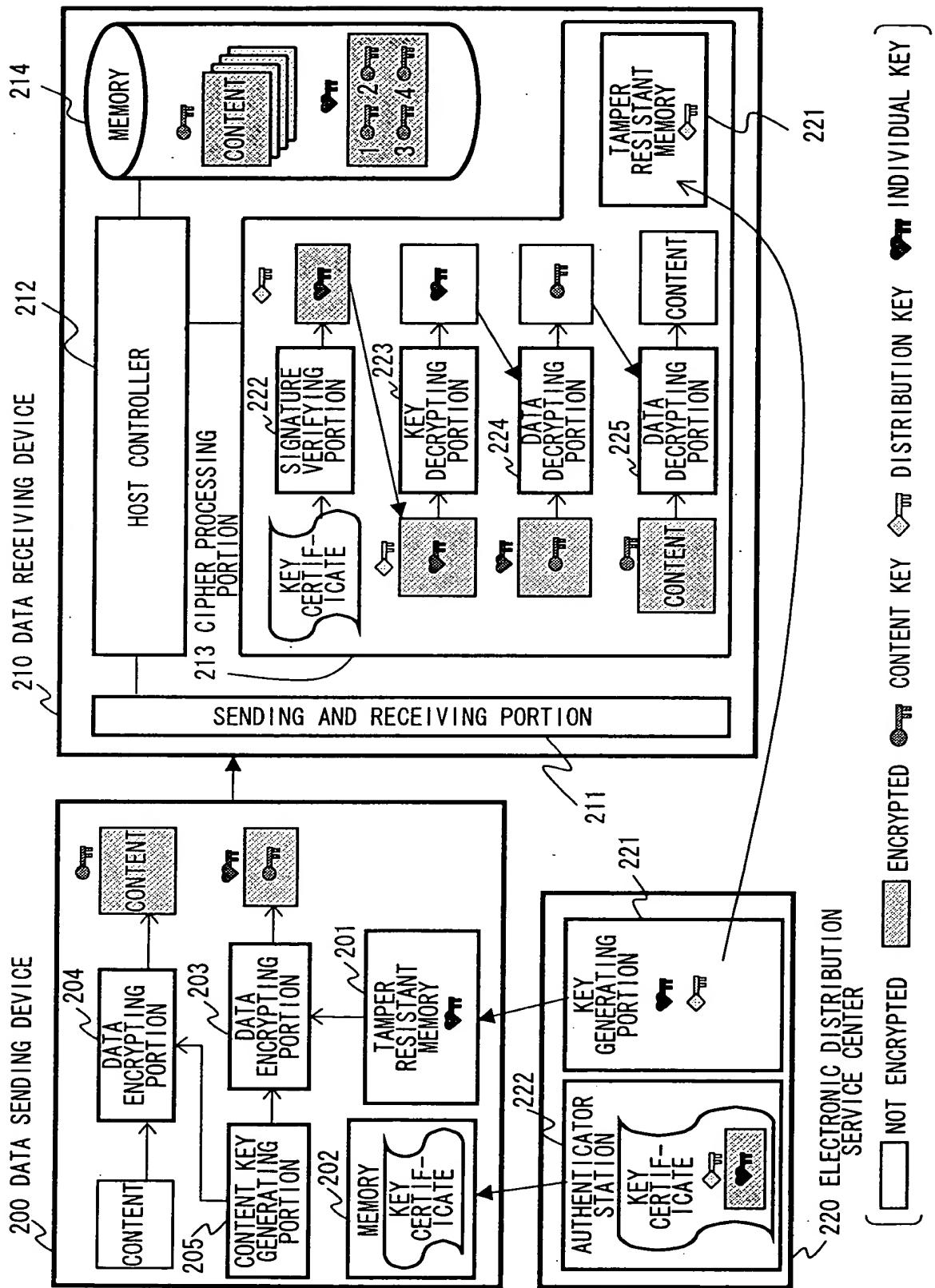


FIG. 85

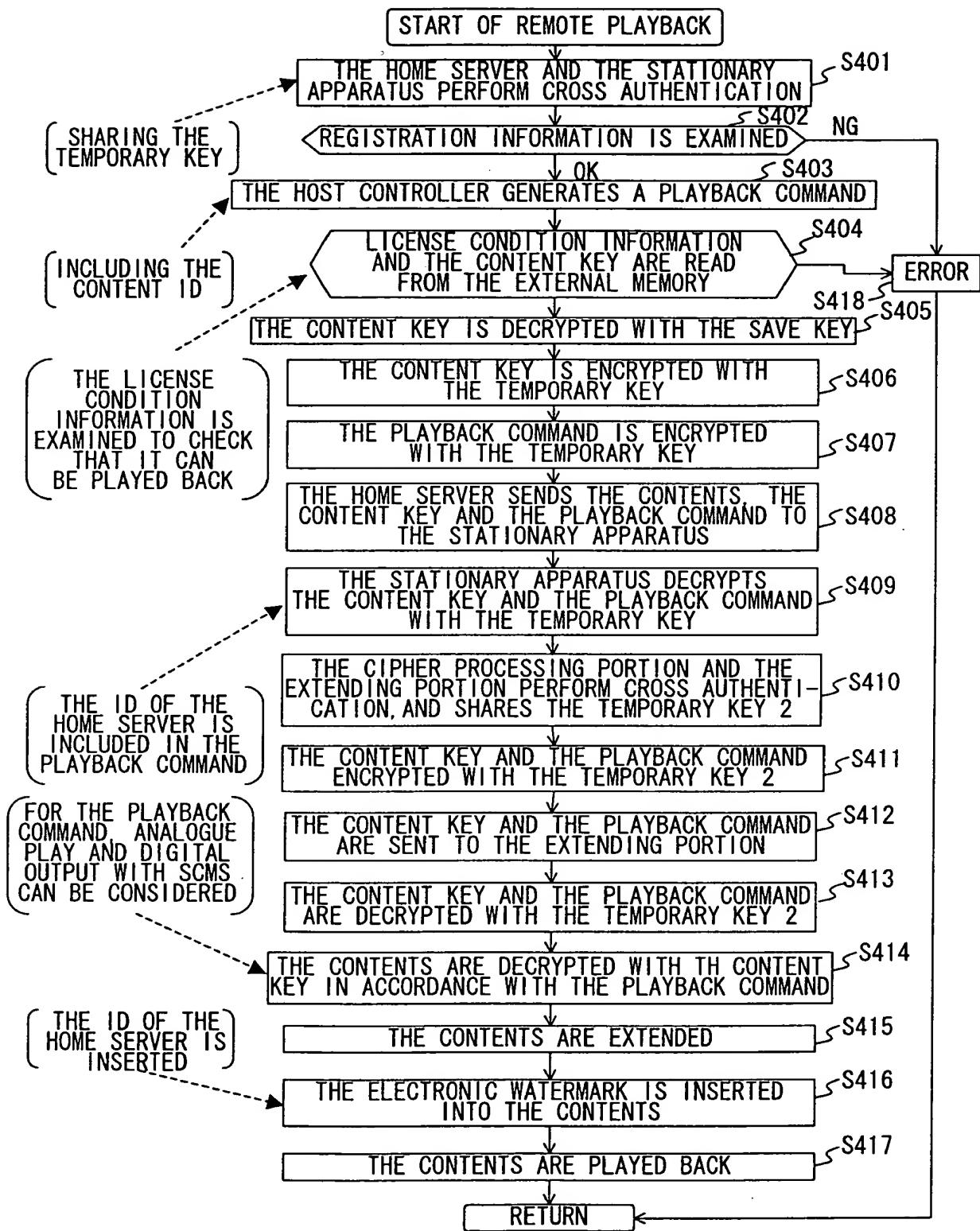


FIG. 86

09/830392

四庫全書

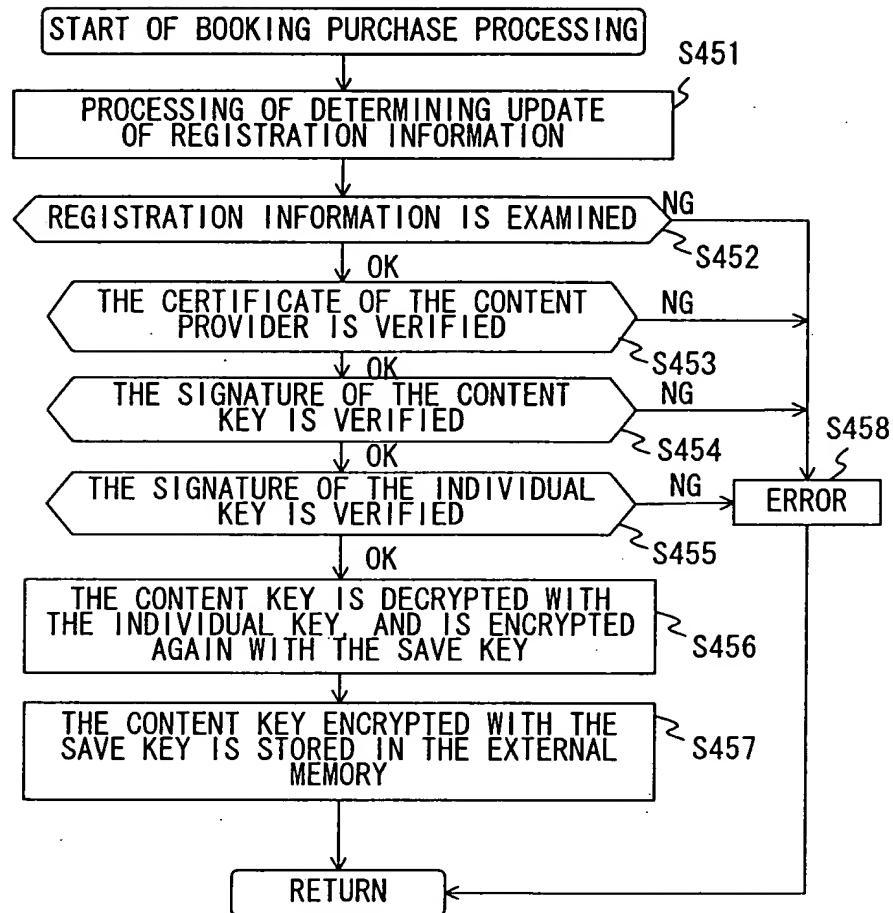


FIG. 87

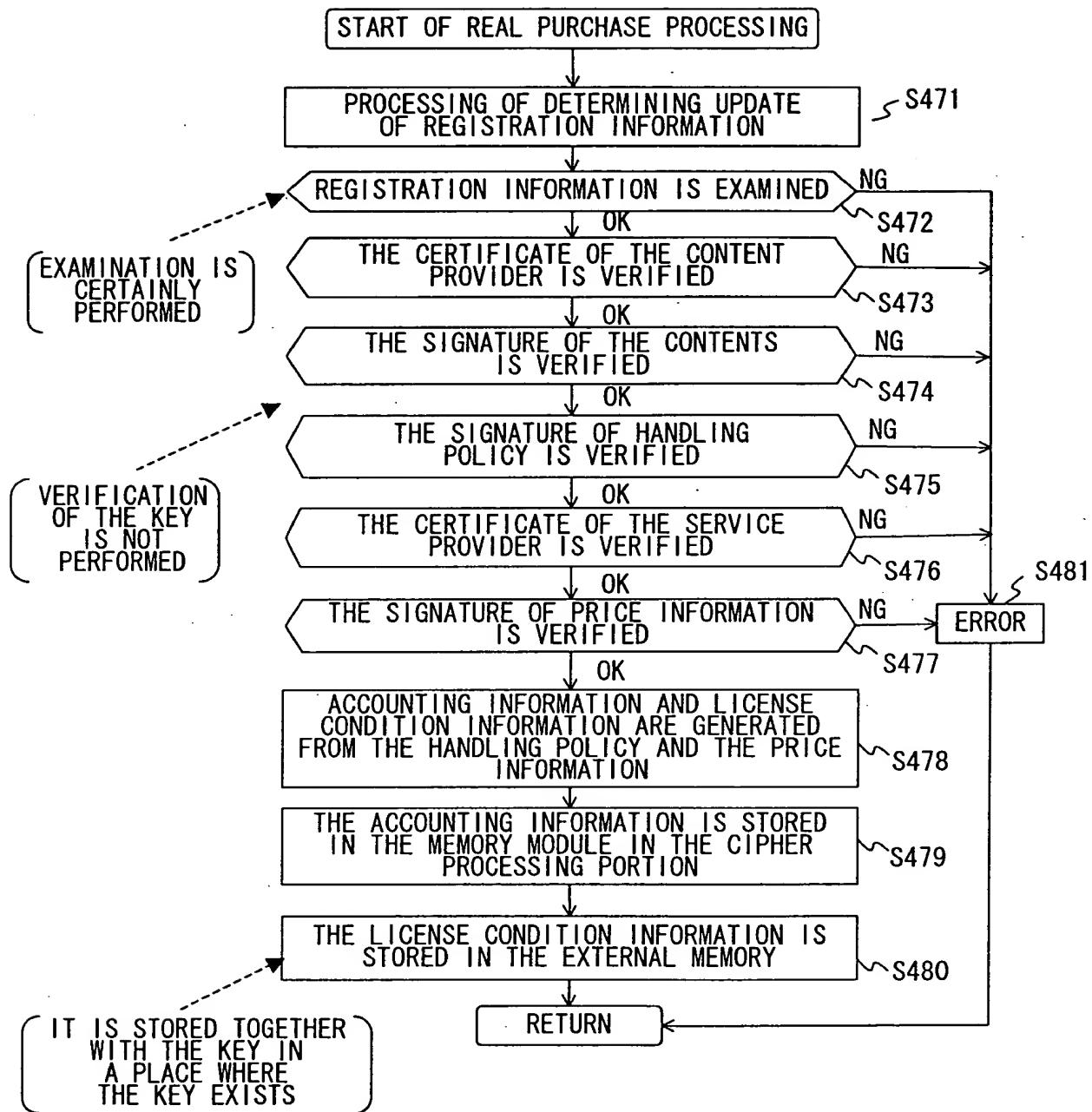


FIG. 88

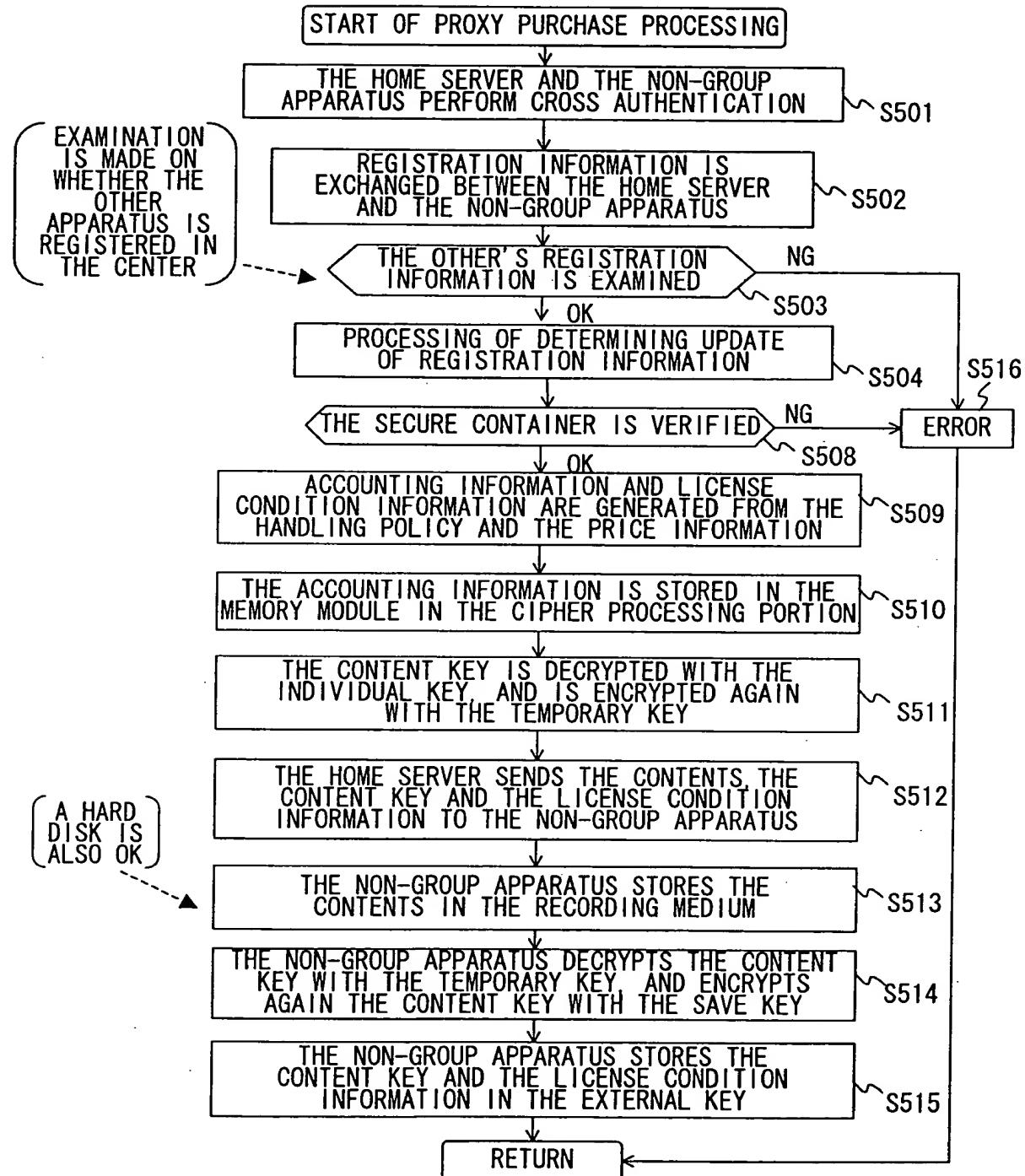


FIG. 89

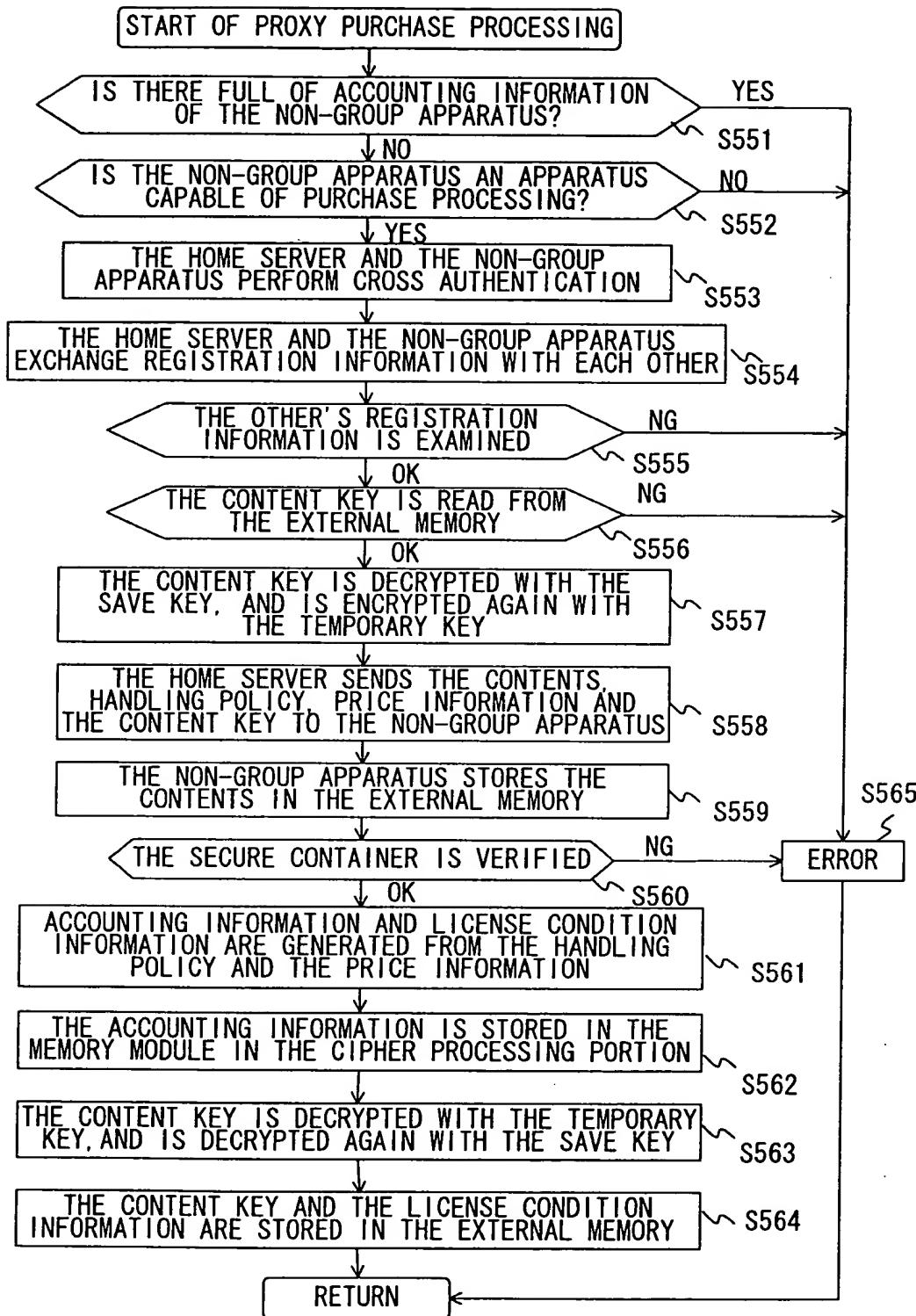


FIG. 90

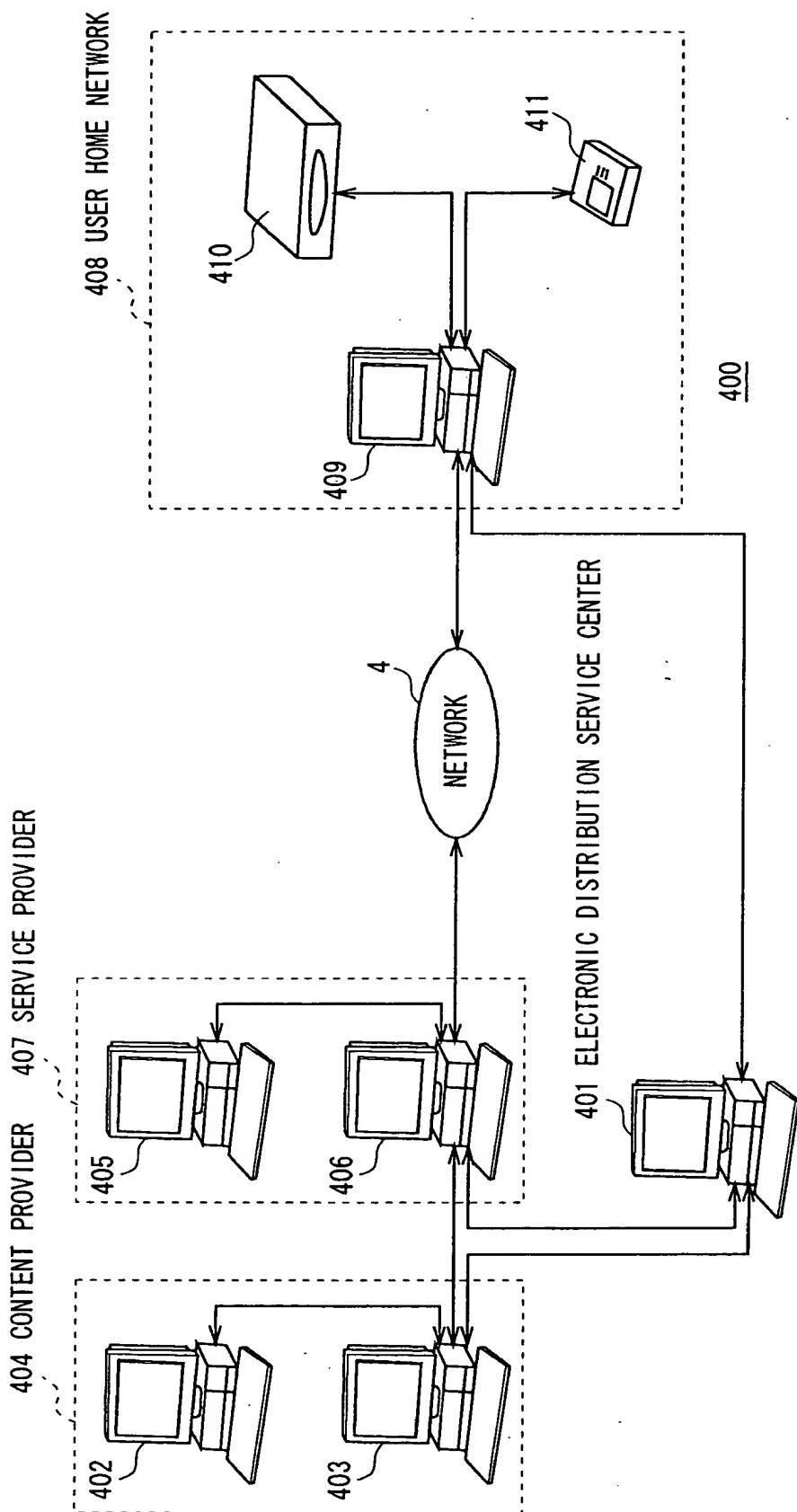


FIG. 91

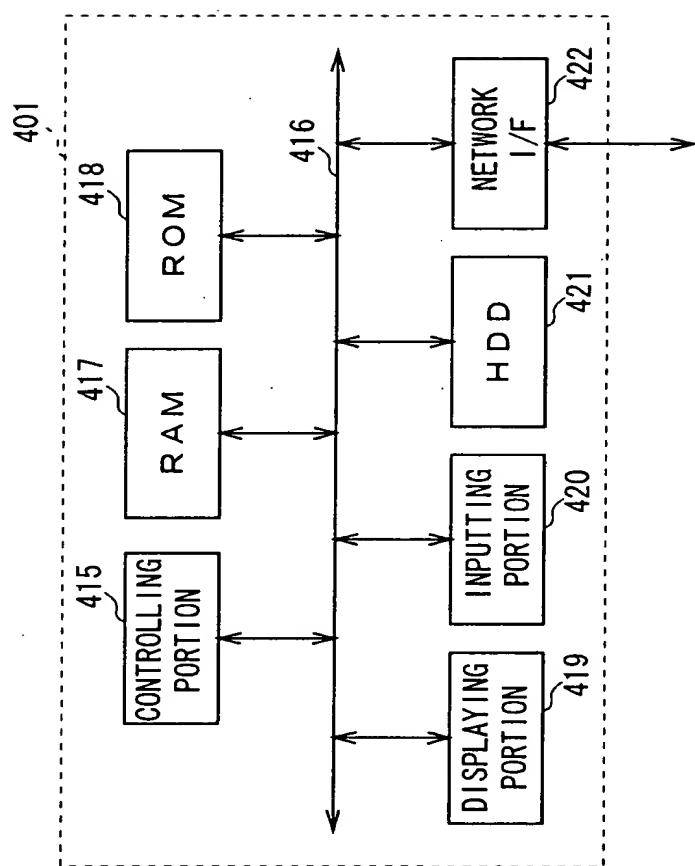


FIG. 92

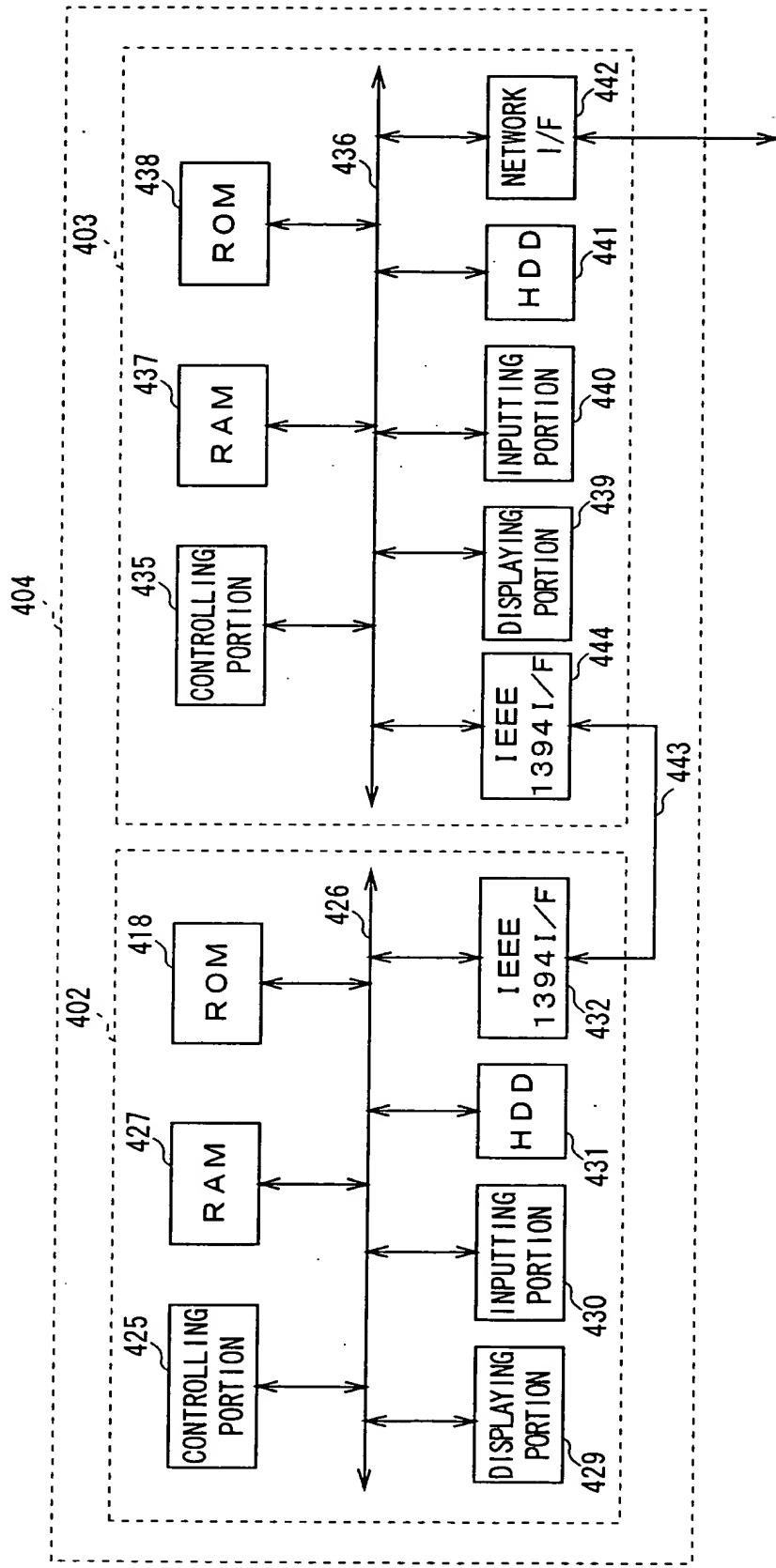


FIG. 93

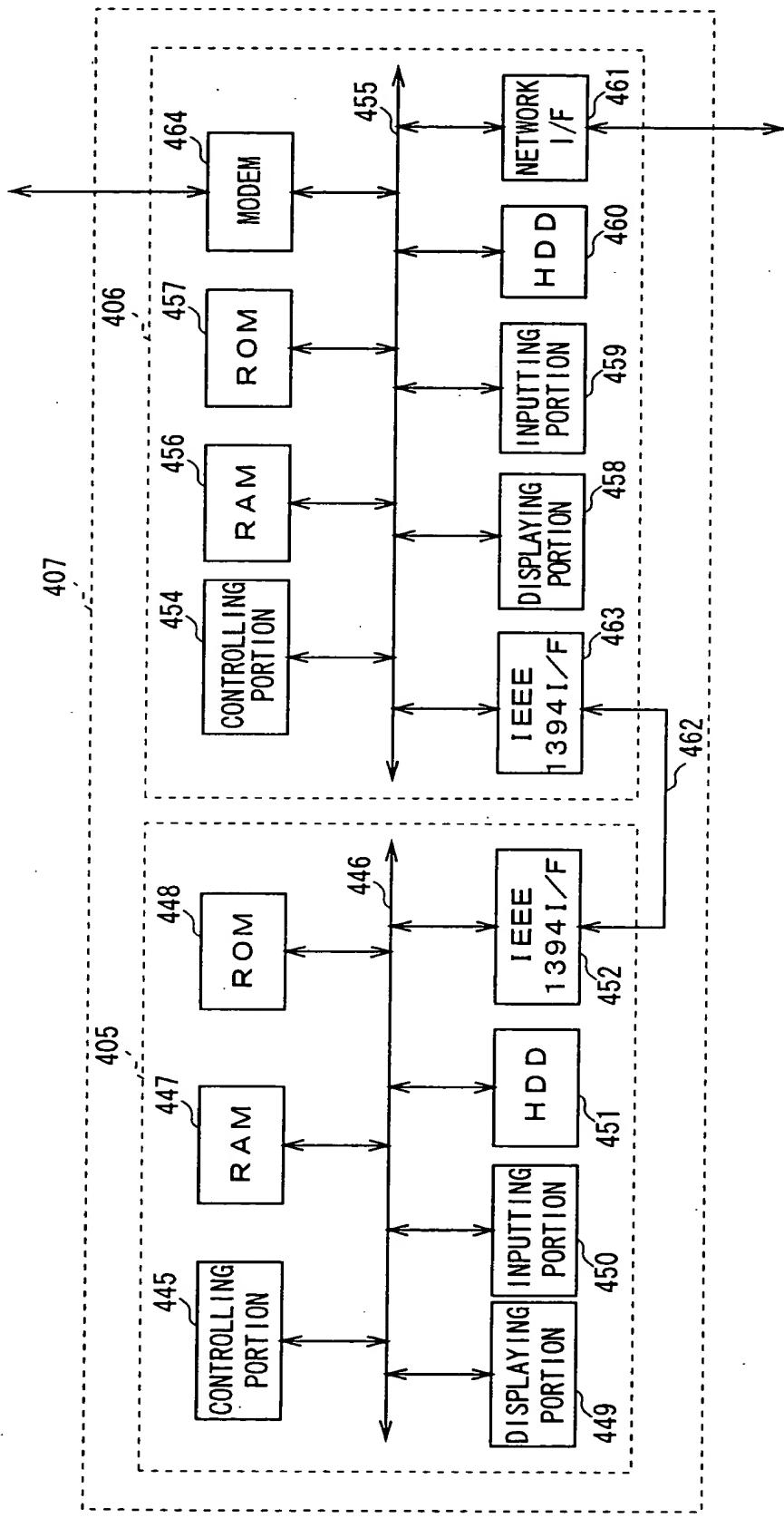
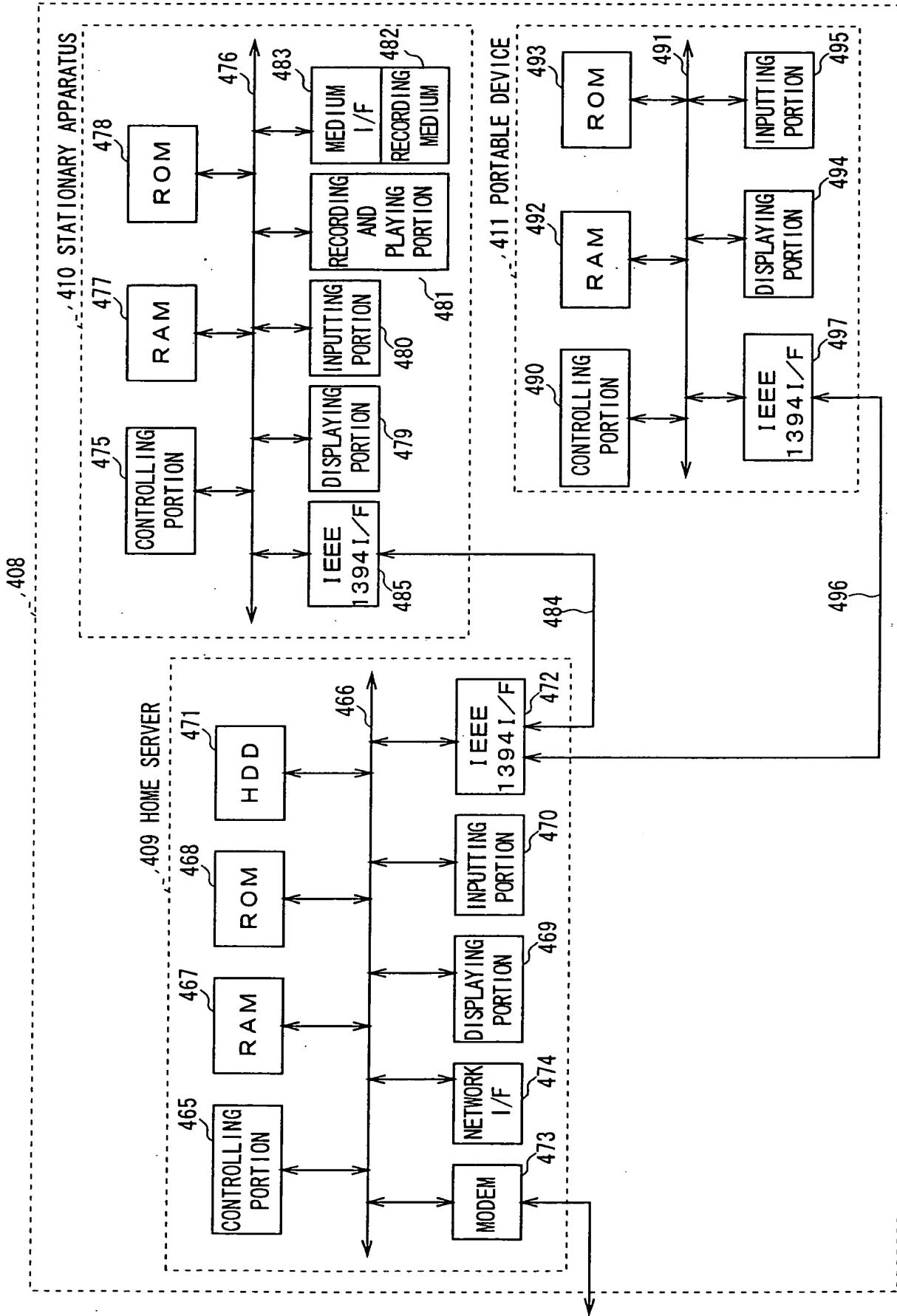


FIG. 94



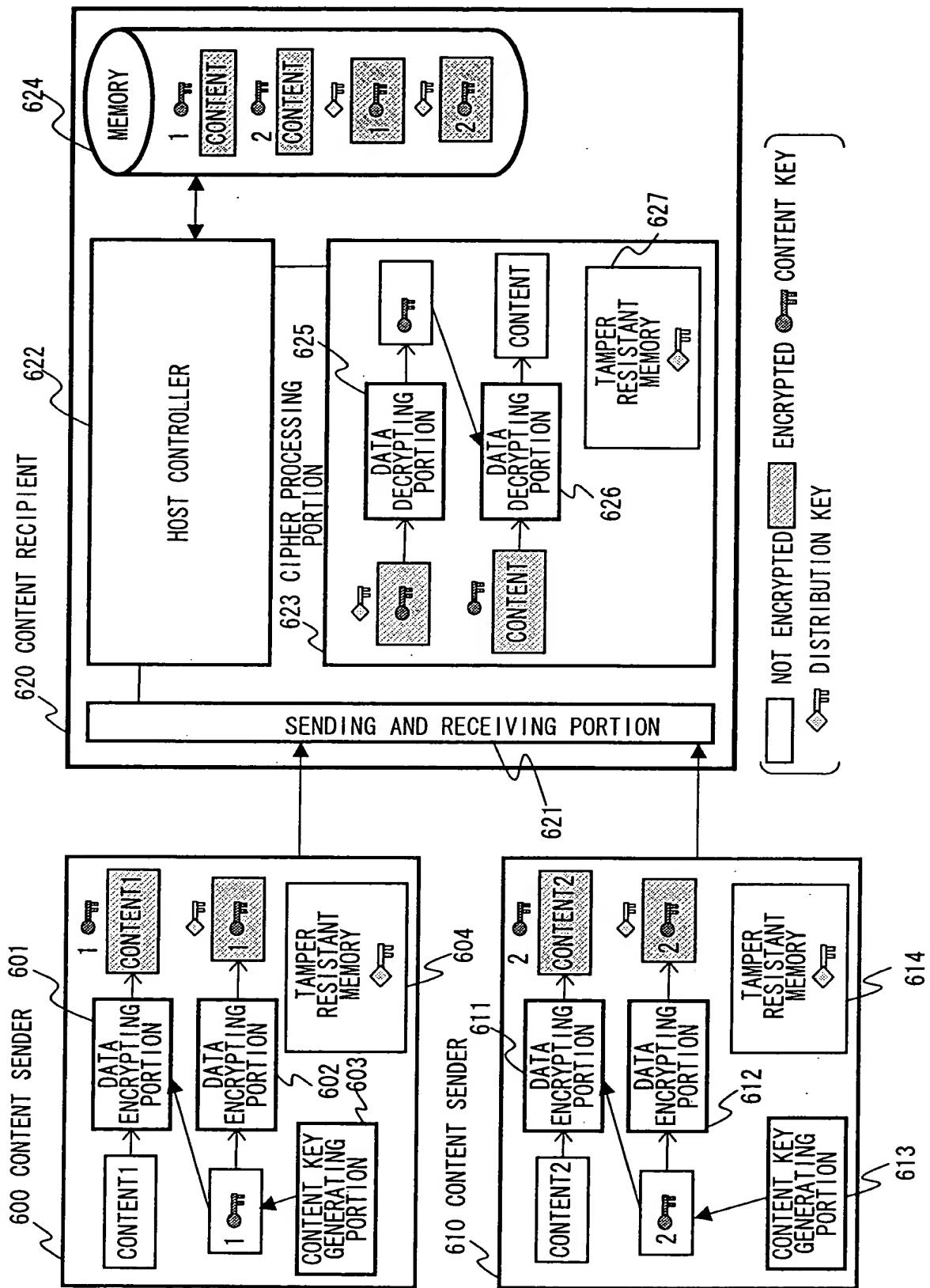


FIG. 96

## Explanation of Reference Numerals

1, 401...electronic distribution service center, 2, 404...content provider, 3, 407...service provider, 4...network, 5, 408...user home network, 10, 400...electronic music distribution system, 11...service provider managing portion, 12...content provider managing portion, 13...copyright managing portion, 14...key server, 15...background data managing portion, 16...benefit distributing portion, 17...cross authenticating portion, 18...user managing portion, 19...account charging portion, 20...banking portion, 21...auditing portion, 22...authenticator station, 23...content server, 24...content authoring portion, 31...content server, 32...electronic water adding portion, 34...content encrypting portion, 35...content key generating portion, 36...content key encrypting portion, 37...handling policy generating portion, 38...signature generating portion, 39...cross authenticating portion, 41...content server, 42...certificate verifying portion, 43...signature verifying portion, 44...pricing portion, 45...signature generating portion, 46...cross authenticating portion, 51, 409...home server, 52, 410...stationary apparatus, 53, 411...portable device, 62, 72, 82...host controller, 56, 73, 83...cipher processing portion, 66, 74, 84...extending portion, 67, 79, 85...external memory, 120...electronic distribution only recording medium, 402, 405...personal computer for servers, 403, 406...signal processing personal computer